Australian Safety Critical Systems Club

A National Special Interest Group of the

Newsletter

AUSTRALIAN COMPUTER SOCIETY

June 2005

From the Chair

In the last six months, the Club Committee has been very active arranging the 2005 Workshop and hosting courses:

- A five day course Introduction to System Safety Engineering and Management in association with the Australian National University in Canberra. The course was presented by Dr David Pumfrey, University of York.
- A one day Brisbane course in Designing, Documenting, Inspecting and Testing Critical Software presented by Prof David Parnas, University of Limerick;
- A half-day Canberra course in Designing, Documenting, Inspecting and Testing Critical Software presented by Prof David Parnas. (This course was included in the five day course - Introduction to System Safety Engineering and Management.)

There has been an addition to the Club Committee. Westinghouse Signals Australia (now a division of Invensys Rail Systems Australia) has renewed their long standing committee participation after a brief lapse with their nomination of Alex Moffatt. On behalf of the Club, I would like to thank Invensys for their continued support and welcome Alex to the committee. Westinghouse Signals Australia's participation goes back to the formation of the ACS National Technical Committee on Safety Critical Systems in 1992.

George Nikandros
National Chairman

Club Matters

Annual General Meeting

The 2005/06 Annual General Meeting will be held on Thursday, 25 August 2005 in conjunction with the 2005 Workshop at the Corus Hotel, 7-9 York Street, Sydney.

The meeting will commence 5:15pm.

Continues Page 2

10th Australian Workshop

SYDNEY, 25-26 August 2005

Corus Hotel, 7-9 York Street

TOOLS and STANDARDS FOR SAFETY ASSURANCE

The Australian Safety Critical Systems Club announces its 10th National Workshop on Safety Related Systems. The 2005 workshop will be held in Sydney and will focus on two themes:

Theme A: TOOLS for Safety Assurance (including tools used for security and mission-critical systems)

Theme B: STANDARDS (incl. updates to MIL-STD 882E, DefAust) 5679, UK DefStan 00-56 and IEC 61508)

As with the successful 9th Workshop in Brisbane in 2004, a number of international Keynote Speakers will address these topical issues.

Ron Bell
UK Health & Safety Executive. (Project leader for the revision of IEC 61508)

Viv Hamilton
Viv Hamilton Associates Limited
(An author of the new Defence Standard 00-56)

Connie Heitmeyer
USA Naval Research Laboratory's (NRL)
(Principal designer of NRL's SCR (Software Cost Reduction) toolset)

Rod Chapman
Praxis High Integrity Systems, UK

Questions? More Information?

Dr Tony Cant (Program Chair)
Trusted Computer Systems Group
Information Networks Division
Defence Science and Technology Organisation
PO Box 1500, Edinburgh SA 5111 Australia
Phone: +61 8 8259 6700, Fax: +61 8 8259 5589
Mobile: (0412) 348 367,
Email: Tony.Cant@dsto.defence.gov.au

Mr Kevin Anderson (Workshop Chair)
Risk & Reliability Associates Pty Ltd
Level 1, 55 Hardware Lane
Melbourne VIC 3000 Australia
Tel: +61 (0)3 8631 3400 Fax +61 (0)3 9670 6360
Mobile: (0412) 297 822
Email: kevin.anderson@r2a.com.au

See Page 3 for more details

Club Matters (continued)

Club Membership

Club membership has grown significantly since December 2004. It now stands at 78 (an increase of 22). The increase is largely due to the Club's policy of offering an attractive discount to members participating in the Club's events and allowing participants to become members when registering for these events. It will be interesting how many will renew their membership for 2005/06.

Membership renewal notices for 2005/06 will be issued in July 2005.

National Committee

George Nikandros	Chairman
Kevin Anderson	Secretary
Chris Edwards	Treasurer
Tony Cant	Workshop Program Chair
Clive Boughton	Certification & Canberra Chapter Chairman
Robert Worthington	
Peter Hartfield	
Allan Coxson	
Alex Moffatt	
Web Site	www.safety-club.org.au

The term of the current committee expires 30 June 2005. As per the constitution the 2005/06 chairman is elected by the outgoing committee and all other committee positions are declared vacant. George Nikandros will continue as chairman for 2005/06 and all current committee members have agreed to continue.

Anyone interested in being a committee member is invited to contact the Club's Chairman by 31 July 2005.

What's in a name?

As reported in the December 2004 Newsletter, there was concern raised at the 2004 Annual General Meeting held on 19 August 2004, that the use of the term "club" was a deterrent to membership and employer support as it does not convey the image of a learned organisation.

Members were invited in the December Newsletter to make their views known to the Club Secretary. No comments have been received to date.

The Committee has been considering not just alternatives for the term "club" but whether the use of the terms "safety critical" is restrictive as it may portray the image that for example mission critical systems would be outside the group's interest.

The Committee is not ready to propose a completely new name for the organisation. However, the Committee has agreed to propose the use of the term "association" in lieu of "club" as this does not conflict with naming convention for groups within the ACS. The change in name will be put to the membership at the 2005 Annual General Meeting.

Sponsorship

The Club sponsored ASWEC 2005 held in Brisbane in 30 March to 01 April 2005. Apart from having the Club's logo prominently displayed, we were able to distribute information about the Club to people in the software engineering industry. It is through this sponsorship that the Club was able to negotiate with Prof David Parnas to provide the training courses in Brisbane and Canberra.

Continues Page 3

Contents

Club Matters (continued)

Website

As reported in December 2005 Newsletter, the Club's website is limited to 10MB and hence is not sufficient to publish workshop presentations. One option that has been investigated is locating the larger resources at a different location.

Through the efforts of Clive Boughton, we have this month received permission to use the web server facilities at the Australian National University. Whilst some access issues need to be resolved, we expect soon to provide access to much more resource information.

Profile within the ACS

The Committee continues to try to raise its profile within the Australian Computer Society (ACS). Whilst the Club is now one of the more successful groups within the ACS, it remains relatively unknown. To be fair the ACS covers the full spectrum of the IT industry and the club has a relatively small membership base.

The Club resides within the ACS under the Computer Science and Software Engineering (CS&SE) Board. The Club had intended to raise this issue at the CS&SE Board meeting scheduled in April 2005. However this meeting was cancelled. The meeting of the CS&SE Board is currently being proposed for July 2005.

Finance

The Club has some $70K in accumulated funds. These funds have accumulated of the last 10 years; 7 of those years as the ACS National Technical Committee on Safety-Critical Systems.

Whilst this may be seen as a significant sum, it would have been much less without the support of the ACS, the committee members' employer organisations and the outstanding successes of the 7th Australian Workshop (Adelaide 2002), and the 5-day course held at the Australian National University in Canberra in 2005. The success of both these events was beyond all expectation.

Despite the success in terms of technical quality of the 2004 Workshop, the event broke even. The associated series of courses held in Brisbane, Canberra and Melbourne were, however, a financial loss, although not great. The costs associated with the 2004 Workshop, excluding the associated course series were $55K. The costs for the 2005 Workshop are expected to be in the order of $60K. The registration fees set are marginally more than for the 2004 workshop; however they remain favourably comparable to fees for equivalent Sydney events.

The committee intends to continue to use these funds for workshops and educational activities. The club administration costs will rise as the reliance on the committee members' employer organisations reduce.

2005 Workshop

Once again the Club will be hosting a workshop along the same lines as the acclaimed workshops of Adelaide (2002) and Brisbane (2004).

The 2005 (10th) workshop - to be held 25-26 August 2005, at the Corus Hotel, Sydney - has two safety assurance themes; tools and standards. The two day programme will include four invited international renowned speakers:

- ***Ron Bell*** – Ron heads the Electrical and Control Systems Group, within the UK Health & Safety Executive. He is a member of the IEE Safety Critical Systems Policy Advisory Group, Chairman of the IEE Residential School on Safety Critical Systems and Chairman of the IEE Functional Safety Professional Network. He is currently project leader for the revision of IEC 61508 and chairs one of the two teams responsible for the revision.

- ***Viv Hamilton*** – Viv is one of the three authors of the new Defence Standard 00-56 and the author of the accompanying software guidance material. She is a consultant with over fifteen years practical experience in developing and justifying safety related software systems. With extensive experience of the practical use of formal methods, she authored Issue 2 of Defence Standard 00-55. She was at the forefront of the introduction of safety cases in defence systems in the UK. She also provided consultancy to the UK Motor Industry Software Reliability Association in producing the Development Guidelines for Vehicle Based Software (the 'MISRA Guidelines').

- ***Connie Heitmeyer*** – Connie is Head of the Software Engineering, USA Naval Research Laboratory's (NRL) Centre for High Assurance Computer Systems. She is the principal designer of NRL's SCR (Software Cost Reduction) toolset, which has been distributed to over 200 organisations in industry, academia, and government.

- ***Rod Chapman*** - Rod is currently products manager at Praxis Critical Systems, leading the design and development of the SPARK language and toolset. Before joining SPARK team, Rod was involved in the implementation high-integrity real-time and embedded systems, including SHOLIS (the first system implemented to the Def Stan 00-55 SIL4 standard), the Lockheed Martin C130J Mission Computer, and the MULTOS CA

Included in the programme is a function on the Thursday evening. This will be an excellent opportunity to network in a relaxed atmosphere.

For registration and programme details, please visit the Club's website at www.safety-club.org.au.

Bullet Trains Faulty Speed Controls

Source: Risks-Forum Digest Monday 18 April 2005 Volume 23: Issue 84 located at:

http://catless.ncl.ac.uk/Risks/23.84.html

Post Date: Sat, 26 Mar 2005 13:38:42
Posted by: Dennis Mullin

[Source: Mainichi Shimbun, Japan, 23 Mar 2005]

Series 300 bullet trains have been running for years with faulty speed control equipment, Central Japan Railway Co. (JR Tokai) officials said.

Automatic Train Control (ATC) devices that prevent Shinkansen trains from exceeding certain speeds have been faulty on the Series 300 trains, with 52 malfunctions reported this year alone.

In one case, a train travelled at 280 kilometres per hour between Shin-Yokohama and Odawara stations in Kanagawa Prefecture on March 3, even though the speed limit on the line is 270 kilometres per hour.

JR Tokai says the error came from faulty software supplied by the makers of the devices and that the glitch was not even detected during test runs.

Land, Infrastructure and Transport Ministry officials have asked JR Tokai to provide a complete explanation of the case.

JR Tokai said one of the cases involved a Series 300 bullet train driver being forced to reduce speed manually after the ATC on the train he was driving on March 19 failed to work.

A check of the ATC later revealed that software supposed to detect train speeds was not working properly. This caused the ATC to estimate the train was travelling slower than it actually was.

JR Tokai has stopped using the faulty equipment.

Prius cars shutdown at speed

Source: Risks-Forum Digest Tuesday 17 May 2005 Volume 23: Issue 87 located at:

http://catless.ncl.ac.uk/Risks/23.87.html

Post Date: Tue, 17 May 2005 13:19:35 +0300
Posted By: "Edwin Slonim"

The U.S. National Highway Transportation Safety Administration has 13 reports of Toyota's Prius gas-electric hybrid cars (2004 and early 2005) stalling or shutting down at highway-driving speeds, which Toyota attributes to software problems. [Source: Toyota Attributes Prius Shutdowns To Software Glitch - Sholnn Freeman, *The Wall Street Journal*, 16 May 2005; PGN-ed]

I have always feared losing power, brakes and steering at high speed – with a helpful dashboard indication of "internal error 687, please reset". Looks like it is starting to happen. Of course we need to put this into proportion - how many cars stall at high speed with a fuel blockage, or swerve with a blow out.

Education - Safety Critical Systems

For some time now the Club has been attempting to develop a specialist subject unit relating to safety-critical systems as part of the ACS Certification Program (CMACS). Despite the Club's endeavours and the initial enthusiasm by those responsible for the CMACS program, there has yet to be any progress on the matter by CMACS. Current indications are that the CMACS unit will not happen. The Club will now investigate other possible certification options.

However the Club, in conjunction with the Australian National University (ANU) ran a 40 hour Introduction to System Safety Engineering and Management course in April 2005 at ANU. The course is the course developed by the University of York and was presented by Dr David Pumfrey with the assistance of Kevin Anderson, Dr Clive Boughton, Gordon Stone and Malcolm Newey. There were 24 course attendees of which 10 were Masters Degree students and 14 from industry.

There were no prerequisites for participation.

The success of the course has encouraged the Club to run it again in April 2006 (see advert). Those wishing to participate should contact the Club Secretary.

Event Reports

2004 Workshop

The papers for the 9th Australian Workshop on Safety Critical Systems held in Brisbane on 19-20 August 2004 have been published and are available at the ACS Conferences in Research and Practice in Information Technology website (http://crpit.com/Vol47.html).

Hard copies will be distributed to financial members.

David Parnas Courses

Prof David Parnas, internationally renowned for his influence on software design and development and the author of more than 200 papers and reports, was an invited speaker to ASWEC 2005. Having someone of David's repute in Australia was an opportunity the Club

could not pass up and negotiated with David to deliver a one day Brisbane course and a half-day Canberra course titled Designing, Documenting, Inspecting and Testing Critical Software.

Topics covered in the course included:

- General principles for reducing complexity
- Systematic documentation of system requirements
- Architecture design
- Inspecting of design documents and code
- Testing for reliability assessment.

The attendances at the courses were Brisbane 21 and Canberra 35. The Canberra attendees include the 24 participants in the Introduction to System Safety Engineering and Management course.

Canberra Chapter

Mike Brown is a Senior Technical Specialist with EG&G and has a long and distinguished career in systems safety engineering and education.

The ITE&E Branch of Engineer's Australia in Canberra arranged for Mike Brown to give a seminar which he titled "System Safety Engineering: Professional Engineering, Professional Pessimism or What?" The Club's Canberra chapter members were invited to participate. Mike's presentation, held on 19 April 2005 at Engineering House, centred on discussing all the sorts of issues, the sometimes confusing/conflicting standards and contexts, and the tensions that occur between professional engineers and professional safety system engineers when dealing with highly safety critical systems. The seminar was well received by an audience ranging from university students to very experienced government and industry systems safety practitioners.

After the meeting Ian Noble (representing ITE&E Branch of EA), Clive Boughton (representing aSCSc) and Malcolm Newey (ANU) accompanied Mike Brown, his wife Beverly, and his colleagues Ludwig Sorrentino and Marilyn Eichelberger to a dinner at the Brassey Hotel.

Bulletin Boards

ACM Risk Forum On Risks To The Public In Computers and Related Systems – http://catless.ncl.ac.uk/Risks.

Safety-Critical Mailing List Forum hosted by the University of York. Need to join using the form located at www.cs.york.ac.uk/hise/text/sclist/form.php for access.

Introduction to System Safety Engineering and Management
(Content to be confirmed)

Day 1	• Introduction and Safety Concepts • Development for Safety • Preliminary Hazard Identification & Case Study • Modelling Event Sequences • Case Study: Chemical Containment Fault Tree • Risk Assessment
Day 2	• Functional Hazard Assessment • Case Study: ARP4761 WBS FHA • HAZOP • Case Study: Process Plant HAZOP • Systematic failure • Safety Integrity levels
Day 3	• Safety Analysis techniques 1 • Case Study: AGV Fault Tree and FMEA • Safety Cases 1 • Case Study: Safety Case Construction • Safety Cases 2
Day 4	• Safety Analysis Techniques 2 • Preliminary System Safety Assessment • Case Study: ARP 4761 WBS PSSA and SSA review • Common Cause Analysis • Safety case: Common Causes • Introduction to Software Safety
Day 5	• Safety Management • Case Study: AGV Safety Management • Human factors • Safety Culture • Conclusions • Bibliography • Glossary

Australian National University
April 2006

Registration
(to be advised)

Contact Club Secretary to register interest and for more information

Early bird and group (5 or more) discounts