Australian Safety Critical Systems Club
A National Special Interest Group of the Australian Computer Society

Newsletter

December 2004

From the Chair

It has been some time since the last newsletter (August 2003), our first in fact. For this I apologise. Our goal is to publish a quarterly newsletter, but this very much depends on having sufficient content. We welcome items that have some relation to safety-related systems containing software. If you have any items of interest, please share them by forwarding them to the Club Secretary.

In the period since the last newsletter, the Club has been very active in hosting two workshops; Canberra (October 2003) and Brisbane (August 2004) and progressing the development of a course module in relation to safety-critical systems to be offered as part of the ACS Member Certification Program (CMACS). It is anticipated that a course will be held in April 2005. Planning for the next workshop to be held in Sydney in August 2005 is underway.

Club membership is growing, albeit slowly. Membership is currently 56. Including the option to join the Club on the workshop registration form thus allowing those who take up the option to avail themselves of member discounts is very successful, with some 80% of registrations taking up the offer. However sustaining memberships from year to year has not been as successful. One factor is that people tend to move on rather frequently – this seems to be a reflection of the general volatility of the IT industry.

The Club Committee membership has undergone change. Peter Lindsay, after some 10 years on the ACS National Technical Committee on Safety Critical Systems (that Committee is now the Club Committee), and 2 years as Chairman resigned due to work commitments. Peter however continues to be a member of the Club and supporter of the Club's activities. Jacqui Newbegin, after some 3 years as a committee member, has resigned due to a temporary change in career, namely motherhood. On behalf of the Club Committee and the membership, I thank both Peter and Jacqui for their contribution and wish them well. On the plus side, the committee gained two new members, Peter Hartfield and Robert Worthington.

The Annual General Meeting was held on 19 August 2004 during the Brisbane 2004 Workshop. The committee was re-elected.

George Nikandros
National Chairman

Contents

From the Chair	**1**
Club Matters	**1**
Sod's Law succumbs to Murphy	**2**
Education – Safety Critical Systems	**3**
Software and the law	**4**
Event Reports	**4**
2005 Workshop	**5**

Club Matters

National Committee

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

Club Membership

The Club currently has 56 financial members, most of who joined to attend the 2004 Workshop. The Club has around 200 lapsed memberships. Only a handful of previous members have renewed their membership. Lapsed members can expect a renewal reminder notice in the near future.

Sponsorship

The Club is a Bronze Level sponsor of ASWEC 2005 to be held in Brisbane in March 2005. For more details see http://aswec2005.itee.uq.edu.au/home.php.

Such sponsorships help raise the profile of the Club.

Bulletin Board

The Committee discussed the establishment of a Bulletin Board as a service to the membership. The committee decided not to pursue this initiative for now at least, because for it to be effective there needs to be a very effective moderator – effective in controlling the discussion to avoid abuse and misuse of the service and by devoting the time necessary.

Another factor was existence of some very good bulletin boards e.g.

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.

What's in a name?

At the Annual General Meeting held on 19 August 2004, there was discussion on club membership and event participation. An issue that was raised concerned the use of the term "club". There was an opinion 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.

The use of the term "club" was used to reflect the similar organisation in the UK. The committee is seeking the views members on the matter. Please forward your views to the Club Secretary (see www.safety-club.org.au for e-mail contact details).

Website

The Club's website is currently limited to 10MB and hence is not sufficient to publish workshop presentations. The Committee is currently investigating options for increasing capacity. Merely increasing the capacity at the current site is expensive. The committee is investigating the option of locating the larger volumes of data at another location.

The Committee is also trying to raise its profile within the Australian Computer Society (ACS). The Club is currently buried under the CS&SE Board. Although we are a SIG (Special Interest Group) within the ACS, the Club is not listed as such and is generally unknown within the Society.

Sod's Law formula succumbs to Murphy

An article titled "Mathematical formulae predicts your worst moment" was published in the Courier Mail newspaper on 8 October 2004.

It relates to a formula that claims to prove that Sod's Law really does strike at the worst possible time.

The formula is the result of work commissioned by British Gas. According to British Gas [1], a panel of experts, namely a psychologist (Dr David Lewis), a mathematician (Philip Obayda), and an economist (Dr Keylan Leyser) have discovered a statistical formula for predicting Sod's Law occurrences.

The formula published in the Courier Mail article unfortunately did not match the formula as described in the article text (Sod's Law). The article text did however correctly represent the formula as published on the British Gas website.

According to the article and the British Gas website, the experts have now provided a statistically based rule for predicting Sod's Law of "*Anything that can go wrong, will go wrong*". In so doing, they have also discovered a new law "*Things don't just go wrong, they do so at the most annoying moment*".

The British Gas published formula gives the Probability of Sod's Law Occurring and is based on five factors – urgency (U), complexity (C), importance (I), skill (S) and frequency (F). Each of these factors has to be applied to a task or an event, and each scored between 0 and 9. A sixth factor, aggravation (A), was set at 0.7 by the boffins after their polling of 1000 people.

$$\frac{(U+C+I)*(10-S)}{20} * A * \frac{1}{1-SIN(\frac{F}{10})}$$

[British Gas Formula]

According to British Gas the formula enables the scoring of a Sod's Law probability on a scale of 0 to 8.6. Here's where Murphy's Law comes into play. If U, C, I and F have the value 9, and S has the value 1, the result is 34.25 – well above the claimed 8.6 maximum. Something is wrong.

According to the mathematician on the British Gas expert panel, Philip Obayda [2], who, incidentally, is also cited as an architecture student, the formula is not the same as the one he derived His formula is similar except that the factors U, C, I, S and F have values greater than 0 and less than 1, with A still being 0.7. The results of this formula, according to Philip Obadya lie in the range 0 and 1.

$$\frac{(U+C+I)*(1-S)}{2} * A * \frac{1}{1-SIN(F)}$$

[Philip Obayda Formula]

However, if U, C, I and F have the value 0.9, and S has the value 0.1, the result is 3.925 i.e. much greater than the claimed maximum value 1.

It would appear Sod's Law has succumbed to Murphy's Law.

References

[1] British Gas

www.britishgasnews.co.uk/index.asp?PageID=16&Year=2004&NewsID=623

[2] Philip Obayda

www.livingroom.org.au/blog/archives/murphys_law_calculator.php

Education - Safety Critical Systems

The ACS provides a Certification Program (CMACS) which provides a unique professional development opportunity. It is an industry based Masters level course of study which provides participants with:

- High quality and ongoing professional development
- Current and relevant ICT and business knowledge
- Defined benchmarks against which to test professional skills
- Professional recognition of up to date skills and knowledge
- Understanding of ethical standards for the IT profession
- Opportunities to add immediate value to your organisation.

The CMACS Program currently comprises of four units:

- Core Unit 1 – Technology Trends
- Core Unit 2 – Business, Legal and Ethical Issues
- Core Unit 3 – Business, Strategy and IT
- Unit 4 – Specialist Subject selected from Digital Business, e-Learning, Knowledge Management, Managing Technology and Operations, Project Management, Software Development.

The Club is seeking approval for a new specialist unit in Safety Critical Systems. It is proposed for the unit to be constituted as a subject in the Masters in Software Engineering provided by the Australian National University (ANU). The unit is expected to comprise:

- Five days hands-on Introduction to System Safety Engineering and Management (40 hours) based on course materials from the University of York High Integrity Systems Engineering Group (HISE).
- Three assignments (20 hours each).
- On-line education (30 hours).
- One examination (20 hours, includes preparation)

There are a number of issues that remain to be resolved. However it is planned to offer the Introduction to System Safety Engineering and Management (40 hours) part of the unit in April 2005 at ANU.

Continued Page 4

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
Early April 2005

Register Now!

Contact Club Secretary to register interest and for more information

Early bird and group (5 or more) discounts

There are no prerequisites for participation in the Introduction to System Safety Engineering and

Management course i.e. there is no requirement to be registered in the CMACS Program on for the ANU Masters course.

Those wishing to participate should contact the Club Secretary. Those who register their interest before 31 January 2005, will receive an "early bird" discount. Discounts will also apply to groups of five or more.

For more details about the CMACS Program see www.acs.org.au/certification.

Software and the law

Society's tolerance towards "buggy" software is very much contrary to its tolerance to faulty products and services in general. When it comes to software it seems, society is prepared to tolerate defects as long as the software generally provides the functionality expected.

As a consequence of society's complacency in relation to software, law makers have tended to shy aware from the complex issue of software liability.

In an article Beware of Faulty Software published in the Engineers Australia (July 2004), David Neiger, a mechanical engineer and lawyer, provides some valuable insight into the peculiarities of software in relation to the Australian Trade Practices Act and the various State Fair Trading Acts.

Whilst statute law in relation to negligence is clear, in that designers of faulty products are liable for any reasonably foreseeable loss or damage that arises for the use of the products, these laws are not so clear in relation to software – is software a product?

> *"Most cases involving computer software rely upon intellectual property rights such as copyright, patents and design. No one thought of software as a good….."*
>
> *"At first, object code (the 1s and 0s stored in a ROM or on floppy disks) was not thought of as a property at all because the judges did not consider the electrical charges in a ROM or magnetic pulses on a disk to be a "literary work" worthy of protection. However, source code, which could be read by a human was considered to be a literary work and was protected under copyright law. In 1984, after an appeal, the judges were finally convinced that both source and object (machine) code were literary works that could be protected under copyright. This was enshrined in legislation with the Copyright Amendment (Digital Agenda) Act 2000."*

"While computer programs are considered literary works, they are not covered by the same rules of product liability as physical goods or services. The way the law is presently, the vendors license you to use the computer program in accordance with the conditions of the End User Licensing Agreement (EULA) contract."

By making the use of the software conditional on 'voluntary' acceptance of a EULA, liability is effectively transferred from the software vendor to the software end-user. However goods and services involving the use of the software are very much subject to the Trade Practices Act. Further engineering software tools, being 'literary works' would not be regarded as consumer goods, and as such would not have the statutory warranty protection provided by the Trade Practices Act.

David Neiger sums up the issue thus:

> *Ultimately, as engineers, we are responsible for the output of any computer programs, so if your CAD package or machine control software fails and your designs are faulty, you rather than the software vendor will be held liable.*
>
> *If you write software, you impose any conditions you want in your EULA, so you might as well exclude everything. And be particularly careful if you supply goods that rely on software as you may still be liable, even if the software is at fault unless you have negotiated a different contract with the software vendor.*

It follows of course, those procurers who specify (mandate) software packages to be used in relation to the goods and services to be supplied incur liability arising from the use of the software.

Food for thought!

Event Reports

2003 Workshop

The 2003 Australian Workshop on Safety Critical Systems was held in Canberra on 9-10 October 2003 at the Canberra Convention Centre. This was the eighth such workshop.

The workshop followed the successful format used for the 2002 Workshop in Adelaide – a 1_ day workshop preceded by half-day course, provided by ITEE School of The University Of Queensland.

The workshop gave good coverage of government and industry involvement in Safety Critical Systems covering a wide variety of issues. Details of the program can be found at the Club's website.

The keynote speaker was Professor Peter Ladkin, Professor of Computer Networks and Distributed Systems at the University of Bielefeld in Germany. His talk compared various approaches to incident and accident investigation.

The ITEE course was on the Design of Safety Critical Systems and was presented by Simon Connelly.

Attendance at the workshop was 35 slightly less than the 40 average for previous workshops, but well down on the 80 attendees at the 2002 Workshop.

The papers for the workshop are available at the ACS Conferences in Research and Practice in Information Technology website (http://crpit.com/Vol33.html).

2004 Workshop

The 2004 Australian Workshop on Safety Critical Systems was held in Brisbane on 19-20 August 2004 at

the Chifley at Lennons Hotel. This was the ninth such workshop. However unlike previous workshops, this workshop had a theme, namely "Transport – Can We Trust Programmable Technology?

The format of the workshop was also significantly changed in that it was a two-day workshop with four invited (three international) keynote speakers. In association with the workshop a two-day course was provided in Brisbane (16-17 August), Canberra (23-24 August) and Melbourne (26-27 August).

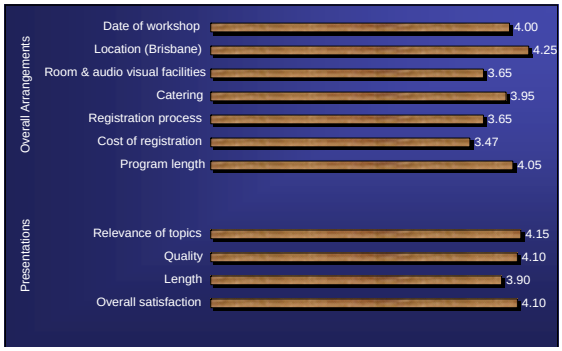
The workshop also received sponsorship from Airsevices Australia and the Defence Materiel Organisation of the Australian Defence Force for which the Club was most grateful.

Details of the program can be found at the Club's website.

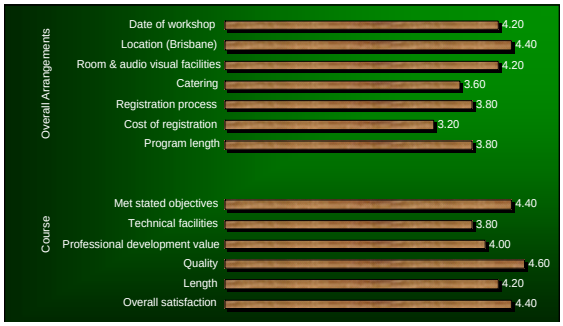
The course was on The Causal Analysis of Critical Systems and was presented by Professor Peter Ladkin, Professor of Computer Networks and Distributed Systems at the University of Bielefeld in Germany.

Attendance at the workshop was 55 more than the 40 average for previous workshops, but well down on the 80 attendees at the 2002 Workshop. This is despite media promotion of the event.

The course attendance was a total of 20, which was down on expectations. However feedback from the workshop and course was very encouraging.



Workshop Delegate Feedback
[Rating range is from 1 (poor) to 5 (excellent)]



Course Delegate Feedback
[Rating range is from 1 (poor) to 5 (excellent)].

The Club has now secured permission to make available the presentation slides from most of the workshop presenters. However the current Club's website space has insufficient capacity to make these available on line. Hopefully this matter will be resolved soon.

The papers for the workshop will eventually be available at the ACS Conferences in Research and Practice in Information Technology website as Volume 38. Expect it around March 2005.

2005 Workshop

10th Australian Workshop

SYDNEY, August 2005 (tentatively 25th and 26th)

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.

Accepted papers will be published in the Australian Computer Society's (ACS) Conferences in Research and Practice in Information Technology (CRPIT) series. CRPIT guidelines should be followed (A4 paper). See http://www.crpit.com for details.

Important dates for authors:

Abstract	11-Mar-05	(text, rtf, MSWord, pdf)
Submission	22-Apr-05	(rtf, MSWord, pdf)
Notice of acceptance	10-Jun-05	
Camera-ready copy	08-Jul-05	(pdf only)

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 3, 225 Clarence Street, Sydney NSW 2000
Phone: +61 2 9249 4613, Fax: +61 2 9262 4110 Mobile: (0412) 297 822, Email: kevin.anderson@r2a.com.au