

The Safety-Critical Systems Club

SSS '11



Safety-critical Systems Symposium 2011

De Vere Grand Harbour Hotel, Southampton

8th - 10th February 2011

The Safety-Critical Systems Club

gratefully acknowledges the support of the following sponsors

BAE Systems

for sponsorship of
the Symposium's proceedings

BAE SYSTEMS

Software Systems Engineering Initiative

for sponsorship of
the Symposium's delegate bags



Programming Research

for sponsorship of
the Symposium banquet



AdaCore

for sponsorship of
the Symposium's banquet pre-dinner drinks



Logica

for sponsorship of
the tools fair



BCS, The Chartered Institute for IT

for overall sponsorship



The Institution of Engineering & Technology

for sponsorship of
the Symposium's technical programme



Further sponsor opportunities are available; please contact Joan Atkinson

Tel: +44 (0) 191 221 2222

Fax: +44 (0) 191 222 7995

THE SAFETY-CRITICAL SYSTEMS CLUB

announces its
Nineteenth Annual

Safety-critical Systems Symposium (SSS '11)

Highlights

Tuesday 8th February:

A whole-day tutorial on

Assurance and Safety Cases

Presented by

Adelard and City University's Centre for Software Reliability

Speakers will include Peter Bishop, Robin Bloomfield, Sofia Guerra, Dan Sheridan, Bev Littlewood and Lorenzo Strigini

Wednesday 9th and Thursday 10th February:

Six sessions of papers, including the following key topics:

- Safety Cases
- Systems Safety in Healthcare
- Technological Matters
- Projects, Services and Systems of Systems
- Testing Safety-Critical Systems
- Safety Standards

Wednesday

An exhibition, and a tools and services fair, will run throughout the day.

Wednesday evening

The Symposium banquet with an after-dinner talk:

Learning about safety by accident

by **Graham Braithwaite,**

Professor of Safety and Accident Investigation at Cranfield University

Society seems gripped by the stories of disaster that are told by accident investigators. Their painstaking assembly of impossible jigsaw puzzles have helped us to understand the complexity of accident causation, but do we really believe everything we read in the newspapers and see on the television? Graham will share some stories about what makes investigators tick. How do they know where to look and how do they react to the unexpected? Should we really be working to make them extinct?

Graham Braithwaite spent the 1990s trying to understand how Australia managed to achieve the enviable record of zero fatalities in commercial jet aircraft crashes; a journey that took him into the effect of culture on safety and which sparked his interest in human and organisational factors. Since 2003 he has worked at Cranfield University, UK, developing and delivering training for accident investigators from around the world working in the transport sectors. He still flies Qantas.

Symposium Attendance

It is possible to attend the tutorial only, the paper sessions only, or both tutorial and paper sessions – with or without accommodation. Please see Page 7 for details.

The Safety-Critical Systems Club welcomes delegates to its Nineteenth annual Symposium

Day 1: Tuesday 8th February 2011

08:30 Registration and *Coffee*

09:30 – 17:00 **Tutorial**

Assurance and Safety Cases

Presented by

Peter Bishop, Robin Bloomfield, Sofia Guerra, Dan Sheridan, Bev Littlewood and Lorenzo Strigini from specialist consultancy **Adelard LLP** and **City University's Centre for Software Reliability**

For many systems we need to know whether the system is secure, reliable or safe enough. We need to communicate, review and debate the trustworthiness of systems with a range of stakeholders, from boardroom to back office and beyond. Assurance and safety cases can be used to justify the adequacy of systems in different applications, including security critical, business critical or service critical. Building a case focuses attention on demonstrating and challenging claims that the system is good enough and involves integrating claims about trusted behaviour, the state of vulnerabilities and compliance with standards.

Over 10 years ago Adelard published the first safety case development manual. It is now working on an updated approach which it intends to make freely available to the safety and assurance community. This is part of our professional response to recent disasters and the Haddon Cave report. We are working with long standing clients to adapt and publish some of the practical work and research.

This day will describe our overall vision and provide technical talks on a range of themes that need to be addressed in a Safety Case manual. There will be presentations from CSR and Adelard covering how to structure cases, justify smart devices, assess diversity, model confidence in claims, and address socio-technical aspects of adaptation and information assurance.

Day 2: Wednesday 9th February 2011

An exhibition and tools and services fair will run throughout the day

09:00 Registration and Coffee

10:00 Introductions

Session 1: **Safety Cases**

10:15 A New Approach to creating Clear Safety Arguments
Richard Hawkins and Tim Kelly, University of York
John Knight and Patrick Graydon, University of Virginia, USA

10:50 Safety Cases – What can we learn from Science?
Steve Kinnersly, ESR Technology

11:25 Accounting for Evidence: managing evidence for goal based software safety standards
Vivien Hamilton, Viv Hamilton Associates Ltd

12:00 Lunch

Session 2: **Projects, Services and Systems of Systems**

13:30 Distinguishing Fact from Fiction in a System of Systems Safety Case
Zoë Stephenson¹, Christian Fairburn², George Despotou¹, Tim Kelly¹, Nicola Herbert²
and Bruce Daughtrey², ¹University of York and ²BAE Systems

14:05 A Project Manager's View of Safety-Critical Systems
Tom Docker, CITI

14:40 System Safety in an IT Service Organization
Mike Parsons and Simon Scutt, Logica

15:15 Tea

Session 3: **Systems Safety in Healthcare**

15:45 Integrating a Risk-based Approach and ISO 62304 into a Quality System for Medical Devices
Celestina Bianco, Systelab Technologies, Spain

16:20 Maintaining the Safety of Operational Health ICT Systems
Alan Debenham, Logica

16:55 Testing of Safety-Critical Software embedded in an Artificial Heart
Sungdeok Cha¹, Sehun Jeong¹, Junbeom Yoo² and Young-Gab Kim¹
¹Korea University and ²Konkuk University, South Korea

19:30 for 20:00 BANQUET with After-dinner talk:

Learning about safety by accident
by **Graham Braithwaite, Professor of Safety and Accident Investigation**
at **Cranfield University**

Day 3: Thursday 10th February 2011

Session 4: **Testing Safety-Critical Systems**

09:00 A Risk Driven Approach to testing Medical Device Software
Albert Farré Benet, Systelab Technologies, Spain

09:35 Testing Experiences of Safety-Critical Embedded Systems
Bryan Bakker, Sioux Embedded Systems, The Netherlands

10:10 Testing of Safety-Critical Systems – a structural approach to test-case design
Armin Beer, Independent Consultant, Bernhard Peischl, Technical University of Graz, Austria

10:45 Coffee

Session 5: **Technological Matters**

11:15 Safety, Security and Multicore
Paul Parkinson, Wind River

11:50 A Pragmatic View of Formal Methods: the Hi-Lite project
Robert Dewar, AdaCore, USA

12:25 Lunch

Session 6: **Safety Standards**

13:45 CE Marking – the Essential Requirements
Mervyn Playle, Quintec

14:20 Introduction and Revision of IEC 61508
Ron Bell, ESC

14:55 Are we there yet? A practitioner's view of DO-178C/ED-12C
Dewi Daniels, Verocel Limited

15:30 Closing Remarks

15:35 Tea and Close of the Symposium

REGISTRATION FEES

The tutorial fee includes lunch on Tuesday and a copy of the handout material from the tutorial. The non-residential symposium fee covers lunch on Wednesday and Thursday, and a copy of the proceedings. A residential option is available which includes accommodation on Wednesday night (with banquet and breakfast) for delegates attending just the two day symposium, or accommodation on Tuesday and Wednesday night (with dinner, banquet and breakfasts) for delegates attending the tutorial and the symposium.

The rates listed below apply to Club members who have paid a current subscription. Non-members, members who have not paid a current subscription, and anyone wishing to renew for 2011 should pay a supplement of **£95** which covers Club membership until 31 December 2011.

	Non-Residential	Residential
Extra night's accommodation	-	£120
Tutorial	£245	-
Symposium only (2 days)	£495	£690
Tutorial & Symposium (3 days)	£695	£995
Membership supplement		£95
Banquet tickets for guests and non-residential delegates		£49 each

VENUE

The symposium will take place at:

Grand Harbour Hotel
West Quay Road, Southampton, SO15 1AG

Tel: + 44 (0) 238 063 3033
Fax: + 44 (0) 238 063 3066

The hotel is situated alongside Southampton's medieval town wall. It has extensive leisure facilities including a gymnasium, sauna, steam room and large swimming pool.

There are daily international flights from Amsterdam, Brussels, Dublin, Dusseldorf and Paris, as well as from several UK airports to Southampton. From Southampton airport to the hotel is a 15 minute taxi journey.

The rail journey from London (Waterloo station) to Southampton (Central station) takes 1hr 15 minutes. It is then a 5 minute taxi ride to the hotel.

By road from the M3, travel south to the M27 westbound; leave the M27 at junction 3 and follow M271 south. At the roundabout at the end of the M271 turn left and follow signs to West Quay.

SYMPOSIUM BANQUET

Dinner on the Wednesday (9th February) will be a symposium banquet in the main suite of the Hotel. The cost of one banquet place is included in the residential packages; additional banquet places can be purchased by all delegates at a cost of £49.

CANCELLATION POLICY

Registration fees paid in advance are refundable (less a £50 cancellation fee) if written notice is received by January 3rd 2011. Refunds cannot be made after this date. All refunds will be issued after the symposium. Delegates are able to replace their attendance with a colleague, but only by notification to the event organiser.

It is very unlikely that the symposium would be cancelled due to adverse weather conditions. We are bound by hotel policies and are still billed for catering and room charges etc. Therefore, we regret that we cannot reimburse delegates in the event of bad weather.

REGISTRATION

A symposium booking form is enclosed with this programme. Requests for further copies of the booking form, or any other enquiries, should be directed to:

Joan Atkinson, Centre for Software Reliability, Claremont Tower, Newcastle University, NE1 7RU, UK

Fax: + 44 191 222 7995 Tel: + 44 191 221 2222 e-mail: Joan.Atkinson@ncl.ac.uk

SCSC

Organised by: Centre for Software Reliability

Supported by: BCS, The Chartered Institute for IT
Institution of Engineering & Technology

Endorsed by: Department for Business,
Innovation & Skills
Engineering and Physical Sciences
Research Council
Health and Safety Executive

CSR

