**THE
SAFETY-CRITICAL SYSTEMS
CLUB
SSS '08**

Safety-critical Systems Symposium 2008

PROGRAMME

Marriott Royal Hotel
Bristol

5th-7th February 2008

The Safety-Critical Systems Club
gratefully acknowledges the support of the following sponsors

BAE Systems

for sponsorship of
the Symposium's proceedings

BAE SYSTEMS

Origin Consulting Ltd.

for sponsorship of
the Tutorial

Praxis High Integrity Systems

for sponsorship of
the delegate bags

Programming Research

for sponsorship of
the Symposium banquet

**The Institution of Engineering
& Technology**

for sponsorship of
the Symposium's technical programme

The Knowledge Network

The British Computer Society

for overall sponsorship

SUPPORTED BY

THE SAFETY-CRITICAL SYSTEMS CLUB

announces its
Sixteenth Annual

Safety-critical Systems Symposium (SSS '08)

Highlights

Tuesday 5th February:

A whole-day tutorial on

Software Safety Case Management

Presented by

Tim Kelly,
*High Integrity Systems Engineering Group,
Department of Computer Science, University of York*

Wednesday 6th and Thursday 7th February:

Six sessions of papers, including the following key topics:

- Themes reprised from SSS '07
- The safety case
- Results of safety-culture initiatives
- Human factors in safety
- Achieving and improving system safety
- Safety and risk analysis

Wednesday

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

Wednesday night

The Symposium banquet with an after-dinner speech:

Courting Disasters
by **Rachel Burnett**, Solicitor and President of the British Computer Society

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 Sixteenth annual Symposium***

Day 1: Tuesday 5th February 2008

08:30 Registration and *Coffee*

09:30 – 17:00 **Software Safety Case Management**

Presented by

Tim Kelly

High Integrity Systems Engineering Group,

Department of Computer Science, University of York

In recent years there has been a marked shift in the regulatory approach to ensuring software safety. Whereas compliance with development standards used to be the norm, the responsibility has now shifted onto the developers and operators to construct and present well reasoned arguments that their software is acceptably safe (in a system context). These arguments (together with supporting evidence) are typically assembled, structured and presented in a software “safety case”.

This tutorial will be of interest to anyone with responsibility for managing, constructing or reviewing software safety cases. Indeed, because the safety case is now considered an integral part of safety engineering and management, the tutorial is crucial to all involved in these disciplines.

The following topics will be covered:

- The role and purpose of the software safety case;
- Approaches to constructing and presenting clear safety arguments (including the Goal Structuring Notation – GSN);
- The current “state of the practice” in preparing software safety cases – in particular, we will discuss the current emphasis on process-based standards and the use of general integrity claims (e.g. Software Integrity Levels);
- The recommended architecture of a software safety case;
- Current work on developing product-based approaches to software safety justification and shifts towards goal-based software safety regulation;
- Managing complexity, change and reuse using modular safety cases.

Day 2: Wednesday 6th February 2008

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

09:00 Registration and *Coffee*

10:05 Introductions

Session 1: Themes Reprised from SSS '07

10:15 Making Safe Software Secure
Odd Nordland, SINTEF ICT, Norway

10:55 Safety Process Improvement with POSE and Alloy
Derek Mannering, General Dynamics UK Ltd., Jon Hall and Lucia Rapanotti, The Open University

11:35 How to Select a Programming Language Subset to Maximise Software Quality
Wojciech Basalaj, Programming Research

12:15 *Lunch*

Session 2: The Safety Case

13:45 Safety Case Development – How can I continue the work?
Tadeusz Cichocki, Dr Tadeusz Cichocki Konsulting, Poland

14:25 Safety Case Experiences from Harrier
Jeff Lucas, BAE Systems

15:05 *Tea*

Session 3: Safety Culture

15:35 Investigation to Establish Whether Cultural Analysis Can Be Used to Improve the Interactions Between Design, Safety and Operations Departments
Tim Smith, T F Smith Ltd

16:15 Human Performance Improvement – Reducing Significant Events in Nuclear Power
Don Goble, British Energy

16:55 *Close*

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

Courting Disasters

by **Rachel Burnett**, *President of the British Computer Society and a Solicitor with her own law firm*

Rachel will speak about safety, quality and legal intervention, referring to legal actions, litigants and lawyers who have helped or hindered the development of the law.

Day 3: Thursday 7th February 2008

Session 4: Human Factors

- 09:00 A Human Factors Perspective On Safety Management Systems
Christopher Lowe, Human Factors Consultant
- 09:40 Human Factors Safety Assurance for Changing ATM Systems
Stephen Clark, Steven Shorrocks and Nic Turley, NATS Ltd
- 10:20 *Coffee*

Session 5: Achieving and Improving System Safety

- 10:50 Practical Ways of Improving Product Safety in Industry
Gabriele Schedl and Werner Winkelbauer, Frequentis AG, Austria
- 11:30 Prototyping versus Formal Development
Mike Ainsworth, Westinghouse Rail Systems Ltd
- 12:10 Systems Approach to Unmanned Air Vehicle Development and Certification
Richard Sleeman, Andrew Cox and Jenny Colledge, BAE Systems
- 12:50 *Lunch*

Session 6: Safety and Risk Analysis

- 14:10 Safety Analysis: Thoughts on Methods and Experience
Michael Ellims, Pi-Shurlok
- 14:50 Simplifying the Creation and Use of the Risk Matrix
Robin Cook, RPS Health, Safety and Environment
- 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 2008 should pay a supplement of **£95** which covers Club membership until 31 December 2008.

	Non-Residential	Residential
Extra night's accommodation	-	£130
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:

Bristol Marriott Royal Hotel
College Green
Bristol, BS1 5TA

Tel: + 44 (0) 117 925 5100
Fax: + 44 (0) 117 925 1515

The hotel is situated in the centre of Bristol, next to the Cathedral. It has extensive leisure facilities including a gymnasium, sauna, steam room and large swimming pool.

There are daily direct international flights to Bristol airport from Amsterdam, Brussels, Frankfurt and Paris, as well as from several UK airports.

The rail journey from London (Paddington) to Bristol (Temple Meads) takes approximately 1 hour and 45 minutes, and then 10 minutes by taxi to the hotel.

SYMPOSIUM BANQUET

Dinner on the Wednesday (6th 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.

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

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

SCSC

Organised by: Centre for Software Reliability

Supported by: British Computer Society
Institution of Engineering & Technology

Endorsed by: Department of Trade and Industry
Engineering and Physical Sciences
Research Council
Health and Safety Executive

CSR

SUPPORTED BY

The Knowledge Network