25th Safety-critical Systems Symposium

S S S

SSS'17 Programme

Bristol Royal Marriott Hotel

7-9 February 2017

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

.

The Safety-Critical Systems Club
invites delegates to its Twenty-Fifth annual Symposium

Safety is increasingly important with autonomous, distributed, highly inter-connected systems all around us, taking over many functions previously done by humans. The world of driverless vehicles, remotely controlled home systems and delivery by drone is happening now.

The Safety-Critical Systems Club has operated in support of our colleagues in the safety community since 1991. Each year, in early February, we have held the Club's annual symposium – SSS. This document provides the programme for the **25th Club Silver Jubilee Symposium in February 2017.**

SSS'17 extends across three full days of presentations, grouped into key themes, in the safety arena. The keynote speakers are: Ron Bell, Robin Bloomfield, Audrey Canning, Dewi Daniels, Les Hatton, Nancy Leveson and John McDermid. There is an invited talk from Harold Thimbleby and a special talk from Tom Anderson. The after-dinner speech will be by Air Marshal Julian Young.

Specific and note-worthy features will be:

- Seven keynote presentations;
- A special talk by Tom Anderson;
- Submitted and invited papers;
- Primary themes of: New Challenges, New Techniques, Software, Safety and Security, Analyses, Data Safety and Accidents;
- Delegate participation throughout, and via a "Practitioners' Question Time" session;
- Tools and services exhibition (Tuesday evening and Wednesday);
- Proceedings volume with full papers for each presentation;
- Version 2.0 of the Data Safety Guidance book;
- Drinks tasting reception on Tuesday evening;
- A "25 at 25" book featuring 25 selected articles from 25 years of the newsletter;
- Symposium banquet, with after-dinner speaker, on the Wednesday evening.

Mike Parsons
Safety-Critical
Systems Club
Event Coordinator

Tim Kelly
Safety-Critical
Systems Club
Director

Bristol Royal Mariott Hotel

Clifton Suspension Bridge

THE SAFETY-CRITICAL SYSTEMS CLUB

announces its Silver Jubilee

Safety-critical Systems Symposium (SSS'17)

Overview

The programme encompasses three days of presentations, seven keynote talks, two special talks, a "Practitioners' Question Time" session and an exhibition.

On the following pages you can read more about the speakers, audience participation, exhibition and social programme, and details of the presentations in the symposium programme.

The papers are grouped into six themes reflecting the broad nature of the symposium. These are: New Challenges, New Techniques, Software, Safety and Security, Analyses and Data Safety.

Tuesday 7th February:

The first day of the Symposium features themes on New Challenges and New Techniques, with eight talks – including our first two keynote presentations:

- Just Playing Catch-Up: The Fate of Safety Engineering?", *John A McDermid*
- Functional safety: Where have we come from, where do we go?, *Audrey Canning*

The afternoon finishes with a special talk from Tom Anderson and an evening reception with canapés and a drinks tasting opportunity (plus alternative refreshments), to be held in the exhibition space.

Wednesday 8th February:

Eight technical papers will be presented on themes of Software and Safety and Security, plus our third and fourth keynote addresses:

- Confidence in a connected world: a safe past and resilient future?, *Robin Bloomfield*
- A Systems Approach to Safety and Cyber-Security: How Far Have We Come?, *Nancy Leveson*

The afternoon finishes with a special session and a lively "Practitioners' Question Time" session. Based on the popular "Gardeners' Question Time" radio programme, this will enable members of the audience to target questions at specific members of the panel.

A tools and services exhibition will run throughout the day.

In the evening, the Symposium banquet dinner features an after-dinner talk from Air Marshal Julian Young, CB OBE

Thursday 9th February:

The third day provides a further nine papers on themes of Analyses, Data Safety and Accidents, including the final three keynote addresses:

- From the IBM 29 Card Punch to the Boeing 787 Dreamliner (and Beyond), *Dewi Daniels*
- A look back at the development of guidelines and standards for safety critical systems over the past 25 years, *Ron Bell*
- Balancing safety with rampant software featuritis, *Les Hatton*

Keynote Speakers

Seven eminent keynote speakers have kindly agreed to contribute to the symposium programme. These keynote speakers are:

Ron Bell, OBE

From 1992 until 2006, Ron Bell was Head of the Electrical and Control Systems Group in HSE. In 1998 he was appointed a member of the Channel Tunnel Safety Authority which is a post he held for 13 years. He chairs one of the two IEC working groups responsible for IEC 61508 (the international standard for functional safety) and in that capacity was responsible for both the first and second editions. In 2005 he received the IEC 1906 Award for his work on functional safety. He is a Royal Academy of Engineering Visiting Professor at Liverpool John Moores University. He is a Director Engineering Safety Consultants Limited.

Robin Bloomfield

Robin is a founder of the specialist safety and security consultancy Adelard LLP. He is also Professor of System and Software Dependability at City University London where he leads a project as part of the UK National Research Centre on Trustworthy ICS (RiTICS). His work in safety and security in the past 30 years has combined policy formulation, technical consulting and underpinning research. He was elected a Fellow of the Royal Academy of Engineering in 2014 in recognition of his international leadership in the engineering of safety-critical systems containing software.

Audrey Canning

Audrey is Managing Director of Virkonnen combined with a continuing commitment to delivery of engineering safety cases, management of engineering research projects and development of safety standards at an International level. She is the international convener for the international safety standard for software engineering IEC 61508-3 and the founding chairman of the IET Safety Community. Audrey has an engineering degree from Cambridge and more than 30 years' experience in the development and assessment of advanced computer-based systems used in safety-critical applications.

Dewi Daniels

Dewi is a director at Software Safety Limited and Aeronautique Associates Ltd. He is a highly experienced software engineer specialising in the development and verification of safety-critical and other kinds of high-integrity software. He is a Chartered Engineer and a Member of the British Computer Society and the Institution of Engineering and Technology. Dewi was a member of the DO-178C/ED-12C Editorial Committee and is currently an invited member of the RTCA/EUROCAE Forum on Aeronautical Software. He was one of the developers of the SPARK Examiner, a tool for developing provably correct Ada programs. He has worked on a number of civil and military aircraft, including the Lockheed C-130J, BAE Systems Hawk, Harrier, Tornado, Bombardier Q400, Airbus A330, A340, MRTT, A380 and Boeing 787. He is currently the Chief Software Engineer at Callen-Lenz/SkyCircuits, where he is leading a team that is developing a flight control system for an optionally manned rotorcraft to DO-178C Level A.

Les Hatton

After being awarded the 1987 Conrad Schlumberger award for his work in geophysics, Les switched careers to study software failure. He has published widely and his theoretical and experimental work can be found in Nature, IEEE Transactions on Software Engineering, IEEE Computer, IEEE Computational Science and Engineering and IEEE Software, for which he also co-edits the popular Impact column with Michiel van Genuchten. His 1995 book 'Safer C' helped promote the use of safer language subsets in commercial embedded control systems, at least for a while.

After rummaging in the sadly predictable ruins of software systems for the next 20 years, he finally realised that too few people really care enough about software quality to effect lasting benefit, and gave up in disgust to return to mathematics and tackle more fundamental problems. Since then he has specialised in computational reproducibility in science, and also applications of information theory and statistical physics to software, the known protoeome and similar systems, demonstrating with co-author Greg Warr in 2015 that a discrete conservation principle acts at a deeper level than natural selection in the evolution of proteins, enforcing a number of important structural properties. In 2016, he was finally able to demonstrate as a result that all such systems asymptote to the same length distribution.

He is Emeritus Professor of Forensic Software Engineering at Kingston University, London.

Nancy Leveson

Nancy is Professor of Aeronautics and Astronautics and also Professor of Engineering Systems at MIT. She is an elected member of the National Academy of Engineering (NAE). Prof. Leveson conducts research on the topics of system safety, software safety, software and system engineering, and human-computer interaction. In 1999, she received the ACM Allen Newell Award for outstanding computer science research and in 1995 the AIAA Information Systems Award for "developing the field of software safety and for promoting responsible software and system engineering practices where life and property are at stake." In 2005 she received the ACM Sigsoft Outstanding Research Award. She has published over 200 research papers and is author of two books, "Safeware: System Safety and Computers" published in 1995 by Addison-Wesley and "Engineering a Safer World" published in 2012 by MIT Press. She consults extensively in many industries on the ways to prevent accidents.

John McDermid, OBE

John became Professor of Software Engineering at the University of York in 1987. He set up the High Integrity Systems Engineering research group in the Department of Computer Science and was Head of the Department from 2006 to 2012. His research covers a broad range of issues in systems, software and safety engineering, and he works closely with government and industry, e.g. Airbus, BAE Systems, the MoD, QinetiQ, and Rolls-Royce, including working on civil and naval nuclear power. He is author or editor of six books and has published about 400 papers. He has advised companies and government departments on several continents, e.g. advising the US Nuclear Regulatory Commission (NRC) on software safety, and reviewing safety management in the UK Defence maritime sector. He has presented invited keynote talks and tutorials at international conferences in several countries, including Australia, Brazil, China, Germany, Japan, Singapore and the USA. He was elected a Fellow of the Royal Academy of Engineering in 2002 and was awarded an OBE in the 2010 New Year's Honours list.

There is also a special talk from Tom Anderson:

Tom Anderson has been a member of the University of Newcastle upon Tyne for over 50 years, first as a mathematics undergraduate, then a postgraduate student in computing, research associate, lecturer, professor, head of computing, dean of science, and dean of business development. He did manage to steal away for a year with NASA (in Virginia) and for a long warm summer at UCLA. From 1984 to 2012 he was Director of the Centre for Software Reliability (CSR) at Newcastle. His research interests lie in the area of system dependability, with particular emphasis on techniques for tolerating faults; he has over 150 publications. He was General Chair for the international conference DSN 2007 in Edinburgh.
And in 1991 he was awarded the contract to set up a national UK Safety-Critical Systems Club, which is now celebrating its Jubilee 25th Annual Safety-critical Systems Symposium.

After-Dinner Speaker

Air Marshal Julian Young was appointed Chief of Materiel (Air) within DE&S in April 2016. In this role he leads an organization of some 1,600 military and civilian staff with the responsibility of spending an annual budget of around £4Bn on equipping and supporting all of the Ministry of Defence's fixed-wing aircraft. He is also the focal point of contact within DE&S for the Royal Air Force, is a Member of the Air Force Board and Chief Engineer (RAF). He also has a MOD-wide role as the Defence Engineering Champion.

Previously, he was DE&S's Director Helicopters for some 16 months, where he was responsible for equipping and supporting Defence's rotorcraft. Prior to that he was DE&S's Technical Director and Chief Information Officer. He was also the MOD's first Defence Authority for Technical & Quality Assurance. Before this spell in DE&S, he was triple-hatted at HQ Air Command as Executive Officer, Chief Engineer and Chief of Staff Support for 2 years. In 2010 he worked with PwC and EADS for 6 months through the Defence Career Partnering Scheme. On promotion to 2-star rank in August 2009, he was appointed as Director Defence Support Review with responsibility for improving the effectiveness and efficiency of Defence Support; many of the ideas generated - including 'Total Support Force' - have been implemented. He was Assistant Chief of Staff A4 (Logistics & Operational Engineering) at HQ Air Command from February 2007 onwards. He attended the Royal College of Defence Studies 2006 Course. For over 2 years previously he was engaged in change, leading the Air Team in the implementation of the Logistics End-to-End Review's recommendations, including Forward & Depth organizations and Lean techniques to the wider Air Force, and then as Programme Director of the Defence Logistics Transformation Programme. He is an Engineer Officer and early operational tours were on Support Helicopter squadrons, including Operation GRANBY (Gulf War I) and detachments to the Falklands. Later tours focused on Harrier GR7/T10 aircraft, both in the Project Team and operationally. He also has been the RAF lead for Engineering, Safety and Quality Policy and, as the Engineering Trade & Engineer Branch Sponsor, authored the RAF Multi-Skilling, tri-Service Aircraft Trade Convergence papers and the 2009 RAF Engineer Branch Strategy. He served as Station Commander at RAF Cosford in 2002-03, and was awarded his CB in 2013 for work related to RAF organizational change and OBE in 2000 for work related to Harrier support.

He is a Governor of the City of Bath College, a member of the Institution of Engineering & Technology's Membership and Professional Development Board, President of the Minerva Society, the RAF Microlight Flying Association and the Abbey Wood Field Gun Crew and Director of RAF Active magazine.

Vendor Exhibition

The exhibition is open to all delegates, will begin on Tuesday evening and end on Wednesday afternoon. It will enable delegates to meet with a number of vendors, who are involved with a range of safety issues across the system development life-cycle. On Wednesday, coffee breaks and lunch will be served in the exhibition space.

Companies who have booked their exhibition space at the conference, in alphabetical order, are:

AbsInt, AdaCore, Altran, Ansys, Ebeni, Green Hills, Isograph, Phaedrus, Resource Group, Synopsys, Wind River

For exhibition opportunities, please contact Joan Atkinson (email: joan.atkinson@ncl.ac.uk or telephone +44 191 221 2222)

Note that the tasting reception will be held in the exhibition areas on Tuesday evening.

Social Programme

Evening Reception – Tuesday 7th February

After the first day of the Symposium, all delegates should take full advantage of this opportunity to unwind, and socialise with friends and colleagues old and new. Thus our 25th SSS offers a Reception with a difference, combining an informal opportunity to meet our exhibitors with an educational tasting experience. Each exhibition stand will have a different variety of alcoholic drinks available, specially chosen to span the aroma and flavour spectrum; you are invited to visit and sample an appropriate number of these fine beverages.

Canapés will be served, and wine plus soft drinks will, of course, also be available.

(The reception is included in the three-day package for both residential and non-residential delegates.)

Symposium Banquet Dinner – Wednesday 8th February

The Silver Anniversary Banquet Dinner will, as usual, be a fine dining experience, held in the symposium hotel, and preceded (at 7.30 pm) by a short welcoming drinks reception.

The dress code is entirely a matter of personal choice but it has been noted, over past years, that a number of our delegates have taken the opportunity to dress for dinner in fine style – we are pleased to applaud and encourage this practice. So, dinner suits are entirely acceptable, but definitely optional.

In accordance with tradition, diners will look forward to a stimulating after-dinner talk; this year the speaker will be Air Marshal Julian A Young CB OBE, Chief of Materiel (Air) Defence Equipment and Support

(The banquet dinner is included in the conference package for residential delegates only. However, non-residential delegates can purchase tickets, preferably when booking.)

Symposium Programme

	Day 1: Tuesday 7th February 2017	
0900	*Registration and Coffee*	
1000	**Introductions and Welcome**	
1010	**Keynote address** Playing Catch-Up: The Fate of Safety Engineering? *John A McDermid, University of York*	**New Challenges** *Chair: Graham Jolliffe*
1055	The “rise of the machine” and the need for a System-of-Systems safety methodology? *Andy German, Mike Brownsword and Ian Mitchell, Atkins*	
1130	Progress Towards the Assurance of Non-Traditional Software *Rob Ashmore, Elizabeth Lennon, Dstl*	
1205	*Lunch*	
1305	**Keynote address** Functional Safety: Where have we come from? Where are we going? *Audrey Canning, Virkonnen Ltd*	
1350	Going ‘Back to the Future’: Developing safety-critical embedded systems using modern Time-Triggered software architectures *Michael J. Pont, SafeTTy Systems Ltd*	**New Techniques** *Chair: Louise Harney*
1425	Product Integrity Assurance Argument Framework for Vehicle Autonomy *John Birch, Mark Cousen, David Ward, HORIBA MIRA Ltd*	
1500	*Tea*	
1530	Experiences of avionics safety certification of an ARINC 653 RTOS on multi-core processor architecture *Paul Parkinson, Wind River*	
1605	**Special talk, introduced by Tim Kelly** What can I say? *Tom Anderson, Newcastle University*	
1650	**“Birds of a Feather” Session**	
1725- 1900	**Symposium Reception** With drinks tasting, and tools and services exhibition	

Day 2: Wednesday 8th February 2017

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

0900	**Keynote address** Confidence in a connected world: safe, secure, resilient and autonomous *Robin E Bloomfield, Kate Netkachova, Peter Bishop, Adelard LLP and City, University of London*	***Chair:*** *Tim Kelly*
0945	Software Handling of Hardware Errors *Chris Hobbs, QNX Software Systems*	**Software** ***Chair: Dave Banham***
1020	*Coffee and Exhibition*	
1100	Closing the Gap – The Formally Verified Optimizing Compiler CompCert *Daniel Kästner, AbsInt GmbH et al*	
1135	Using Formal Proof to meet Executable Object Code and Coverage Objectives in DO-333 *Nick Tudor, D-RisQ Ltd*	
1210	*Lunch and Exhibition*	
1320	**Keynote address** My 36 Years in System Safety Engineering: Looking Backward, Looking Forward *Nancy Leveson, MIT*	***Chair:*** *Tim Kelly*
1405	From Safety Cases to Security Cases *R D Alexander, R D Hawkins, T P Kelly, University of York*	**Safety and Security** ***Chair: Edith Holland***
1440	Cyber Safety and Security for Reduced Crew Operations (RCO) *Kevin R. Driscoll, Honeywell*	
1515	*Tea and Exhibition*	
1550	Waking up to The Insider as a Safety-Critical Threat *Ryan Meeks and Robert Dickie, Frazer-Nash Consultancy Ltd*	
1625 - 1730	**Practitioners' Question Time** *with questions submitted by the audience*	
1930 for 2000	**BANQUET** *With after-dinner talk by Air Marshal Julian A Young CB OBE* *Chief of Materiel (Air) Defence Equipment and Support*	

	Day 3: Thursday 9th February 2017	
0900	**Keynote address** From the IBM 29 Card Punch to the Boeing 787 Dreamliner (and Beyond) *Dewi Daniels, Software Safety Limited and Aeronautique Associates Limited*	***Chair: Tom Anderson***
0945	Analysis of Effects induced by EM disturbances on COTS Devices, from an EM Security and Functional Safety perspective *José Lopes Esteves, Chaouki Kasmi, FNISA-ANSSI* *Davy Pissoort, KU Leuven* *Keith Armstrong, Cherry Clough Consultants Ltd*	**Analyses** ***Chair: Tom Anderson***
1020	Sneak Path Analysis: Realising the Potential *Steve Gregory, AWE*	
1055	*Coffee*	
1120	HFACS: Helicopter Operations' Safety *José Corrêa de Sá, Freelance*	
1155	Integrating Data into the Safety Assessment Methodology for Defence *Louise Harney, Raytheon UK*	**Data Safety** ***Chair: Eric Bridgstock***
1230	*Lunch*	
1330	Cybersecurity problems in a typical hospital (and probably in all of them) *Harold Thimbleby, Swansea University*	
1405	Data: Your Life in its Hands *Tom Adams, Paul Hampton* *Mike Parsons, NATS Ltd*	
1440	**Keynote address** Safety critical systems - A brief history of the development of guidelines and standards *Ron Bell, Engineering Safety Consultants Ltd*	**Final Words** ***Chair: Tim Kelly***
1525	**Keynote address** Balancing safety with rampant software feature-itis *Les Hatton, Kingston University and Oakwood Computing Associates Ltd*.	
1610	**Closing Remarks**	
1615	*Tea and Close of the Symposium*	

REGISTRATION FEES

The non-residential symposium fee covers lunch on Tuesday, Wednesday and Thursday, the reception on Tuesday evening, and a copy of the proceedings. A residential option is available which also includes accommodation on Tuesday night (with evening reception, dinner and breakfast) and Wednesday night (with conference banquet and breakfast), lunches and a copy of the proceedings.

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 2017 should pay a supplement of **£95** which covers Club membership until 31 December 2017.

Bookings for partial attendance (1 or 2 day) can be accepted. Please contact the Symposium organizer (see bottom of this page) for details.

	Non-Residential	**Residential**
Symposium (3 days)	**£775**	**£1095**
Extra night's accommodation	**-**	**£135**

Membership supplement	**£95**
Banquet tickets for non-residential delegates	**£55 each**

VENUE

The Royal Marriott Hotel		
College Green	Tel:	+ 44 (0) 117 925 5100
Bristol, BS1 5TA	Fax:	+ 44 (0) 117 925 1515

The hotel is situated in the centre of Bristol, near to the cathedral. It has extensive leisure facilities including a gymnasium, sauna, steam room and large swimming pool. The hotel has on-site parking, with spaces allocated on a first come, first served basis.

There are daily direct international flights to Bristol airport from many cities in Europe 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 5 minutes by taxi or a 20 minute walk to the hotel.

SYMPOSIUM BANQUET

Dinner on the Wednesday evening (8th February) will be a symposium banquet in the Palm Court room of the Hotel. The cost of one banquet place is included in the residential packages; additional banquet places can be purchased by delegates at a cost of £55.

CANCELLATION POLICY

Registration fees paid in advance are refundable (less a £50 cancellation fee) if written notice is received by January 6th 2017. 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.

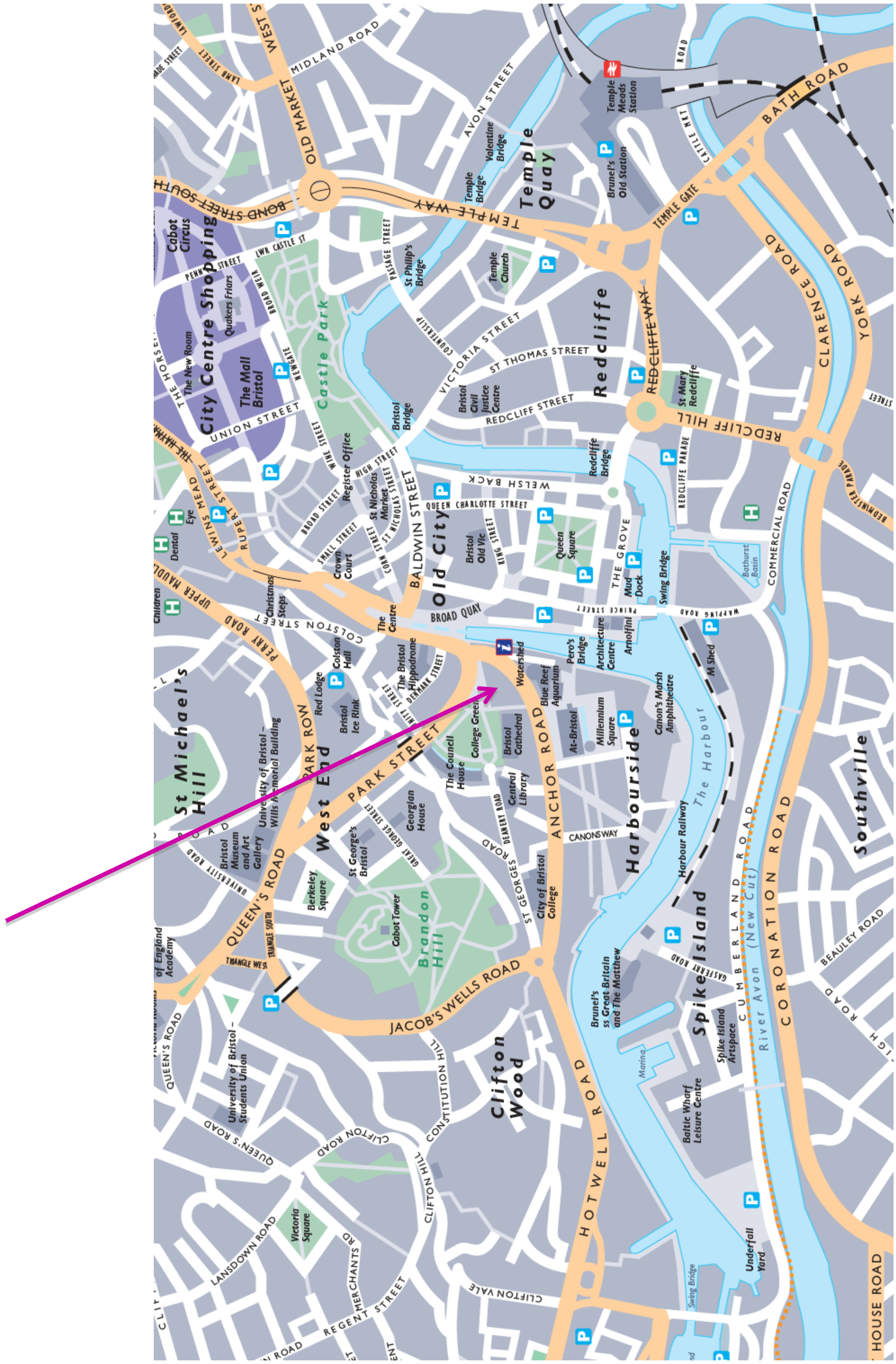
It is extremely unlikely that the symposium would be cancelled due to adverse weather conditions. We are bound by hotel policies and are still billed for catering and room charges, etc. Therefore, we regret that we cannot reimburse delegates in the event of bad weather.

REGISTRATION

All enquiries should be directed to: Alex King, Department of Computer Science, University of York, Deramore Lane, York, YO10 5GH. Phone: 01904 325402 Fax: 01904 325599 Email: alex.king@york.ac.uk

MAP OF BRISTOL

Symposium venue marked with arrow



The Safety-Critical Systems Club wishes to thank everyone who helped to support this event, including:

Event Sponsors

AdaCore
The GNAT Pro Company

Supported By

BAE SYSTEMS

JAGUAR

LAND ROVER

Exhibitors

AbsInt

AdaCore
The GNAT Pro Company

ALTRAN

ANSYS®

Green Hills®
SOFTWARE

ebeni

isograph

PhaedruS
SystemS

resource
group

SYNOPSYS®
Silicon to Software™

WIND™

Endorsed By

bcs
The Chartered Institute for IT

IET The Institution of Engineering and Technology

BIS
Department for Business Innovation & Skills

EPSRC
Engineering and Physical Sciences Research Council

HSE
Health & Safety Executive

Organised by

UNIVERSITY of York

Department of Computer Science, University of York
Phone: 01904 325402 Fax: 01904 325599 Email: alex.king@scsc.uk

The proceedings book is available: ISBN-13: 978-1540796288; ISBN-10: 1540796280