Advances in Systems Safety

Related titles:

Lessons in System Safety
Proceedings of the Eighth Safety-critical Systems Symposium, Southampton, UK, 2000
Redmill and Anderson (Eds)
1-85233-249-2

Aspects of Safety Management
Proceedings of the Ninth Safety-critical Systems Symposium, Bristol, UK, 2001
Redmill and Anderson (Eds)
1-85233-411-8

Components of System Safety
Proceedings of the Tenth Safety-critical Systems Symposium, Southampton, UK, 2002
Redmill and Anderson (Eds)
1-85233-561-0

Current Issues in Safety-critical Systems
Proceedings of the Eleventh Safety-critical Systems Symposium, Bristol, UK, 2003
Redmill and Anderson (Eds)
1-85233-696-X

Practical Elements of Safety
Proceedings of the Twelfth Safety-critical Systems Symposium, Birmingham, UK, 2004
Redmill and Anderson (Eds)
1-85233-800-8

Constituents of Modern System-safety Thinking
Proceedings of the Thirteenth Safety-critical Systems Symposium, Southampton, UK, 2005
Redmill and Anderson (Eds)
1-85233-952-7

Developments in Risk-based Approaches to Safety
Proceedings of the Fourteenth Safety-critical Systems Symposium, Bristol, UK, 2006
Redmill and Anderson (Eds)
1-84628-333-7

The Safety of Systems
Proceedings of the Fifteenth Safety-critical Systems Symposium, Bristol, UK, 2007
Redmill and Anderson (Eds)
978-1-84628-805-0

Improvements in System Safety
Proceedings of the Sixteenth Safety-critical Systems Symposium, Bristol, UK, 2008
Redmill and Anderson (Eds)
978-1-84800-099-5

Safety-Critical Systems: Problems, Process and Practice
Proceedings of the Seventeenth Safety-Critical Systems Symposium, Brighton, UK, 2009
Dale and Anderson (Eds)
978-1-84882-348-8

Making Systems Safer
Proceedings of the Eighteenth Safety-Critical Systems Symposium, Bristol, UK, 2010
Dale and Anderson (Eds)
978-1-84996-085-4

Chris Dale · Tom Anderson
Editors

Advances in Systems Safety

Proceedings of the Nineteenth Safety-Critical Systems Symposium, Southampton, UK, 8–10th February 2011

Safety-Critical
Systems Club

The publication of these proceedings is
sponsored by BAE Systems plc

BAE SYSTEMS

Springer

Editors

Chris Dale
Dale Research Ltd
33 North Street
Martock TA12 6DH
United Kingdom
chris.dale@scsc.org.uk

Prof. Tom Anderson
Centre for Software Reliability
Newcastle University
Newcastle upon Tyne NE1 7RU
United Kingdom

ISBN 978-0-85729-132-5 e-ISBN 978-0-85729-133-2
DOI 10.1007/978-0-85729-133-2
Springer London Dordrecht Heidelberg New York

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The Safety-critical Systems Symposium (SSS), held each February for nineteen consecutive years, offers a full-day tutorial followed by two days of presentations of papers. This book of Proceedings contains all the papers presented at SSS 2011.

The safety case has long been a cornerstone of the discipline, so the Symposium often debates advances in the creation, presentation and management of safety cases, and their associated arguments and evidence. This year is no exception, as will be clear from the three papers in the opening session of the event.

The management of projects developing safety-critical systems poses particular challenges, as do the delivery of systems safety in IT service organisations, and the preparation of safety cases for systems of systems. These important topics are brought together in the second session of the Symposium.

Three papers from healthcare form the third session: one on development processes for medical devices; a second on computer-based operational health systems; and the third on software testing for an artificial heart. The testing theme continues in the fourth session, with three papers on the testing of safety-critical systems.

Technological matters are dealt with in the fifth session: one paper discusses the challenges imposed by the use of multicore processor architectures in critical systems, and the second takes a pragmatic look at the use of formal methods.

The final session picks up on another recurring theme: safety standards. This year, we take a look at CE marking requirements, as well as reviewing significant updates to two important systems safety standards: IEC 61508 and DO-178C.

This year's authors have, as usual, delivered informative material touching on many topics that are of current concern to the safety-critical systems community, and we are grateful to them for their contributions. We also thank our sponsors for their valuable support, and the exhibitors at the Symposium's tools and services fair for their participation. And we thank Joan Atkinson and her team for laying the event's foundation through their exemplary planning and organisation.

CD & TA
October 2010

A message from the sponsors

BAE Systems is pleased to support the publication of these proceedings. We recognise the benefit of the Safety-Critical Systems Club in promoting safety engineering in the UK and value the opportunities provided for continued professional development and the recognition and sharing of good practice. The safety of our employees, those using our products and the general public is critical to our business and is recognised as an important social responsibility.

THE SAFETY-CRITICAL SYSTEMS CLUB

organiser of the

Safety-critical Systems Symposium

What is the Safety-Critical Systems Club?

This 'Community' Club exists to support developers and operators of systems that may have an impact on safety, across all industry sectors. It is an independent, non-profit organisation that co-operates with all bodies involved with safety-critical systems.

Objectives

The Club's two principal objectives are to raise awareness of safety issues in the field of safety-critical systems and to facilitate the transfer of safety technology from wherever it exists.

History

The Club was inaugurated in 1991 under the sponsorship of the UK's Department of Trade and Industry (DTI) and the Engineering and Physical Sciences Research Council (EPSRC). Its secretariat is in the Centre for Software Reliability (CSR) at Newcastle University, and its Meetings Coordinator is Chris Dale of Dale Research Ltd. Felix Redmill of Redmill Consultancy is the Newsletter Editor.

Since 1994 the Club has been self-sufficient, but it retains the active support of the Health and Safety Executive, the Institution of Engineering and Technology, and BCS, the Chartered Institute for IT. All of these bodies are represented on the Club's Steering Group.

The Club's activities

The Club achieves its goals of awareness-raising and technology transfer by focusing on current and emerging practices in safety engineering, software engineering, and standards that relate to safety in processes and products. Its activities include:

- Running the annual Safety-critical Systems Symposium each February (the first was in 1993), with Proceedings published by Springer-Verlag;

- Organising a number of full day seminars each year;
- Providing tutorials on relevant subjects;
- Publishing a newsletter, *Safety Systems*, three times annually (since 1991), in January, May and September; and
- A web-site http://www.scsc.org.uk providing member services, including a safety tools, products and services directory.

Education and communication

The Club brings together technical and managerial personnel within all sectors of the safety-critical-systems community. Its events provide education and training in principles and techniques, and it facilitates the dissemination of lessons within and between industry sectors. It promotes an inter-disciplinary approach to the engineering and management of safety, and it provides a forum for experienced practitioners to meet each other and for the exposure of newcomers to the safety-critical systems industry.

Influence on research

The Club facilitates communication among researchers, the transfer of technology from researchers to users, feedback from users, and the communication of experience between users. It provides a meeting point for industry and academia, a forum for the presentation of the results of relevant projects, and a means of learning and keeping up-to-date in the field.

The Club thus helps to achieve more effective research, a more rapid and effective transfer and use of technology, the identification of best practice, the definition of requirements for education and training, and the dissemination of information. Importantly, it does this within a ‘club’ atmosphere rather than a commercial environment.

Membership

Members pay a reduced fee (well below the commercial level) for events and receive the newsletter and other mailed information. Not being sponsored, the Club depends on members’ subscriptions: these can be paid at the first meeting attended, and are almost always paid by the individual’s employer.

To join, please contact Mrs Joan Atkinson at: The Centre for Software Reliability, Newcastle University, Newcastle upon Tyne, NE1 7RU, UK; Telephone: +44 191 221 2222; Fax: +44 191 222 7995; Email: csr@newcastle.ac.uk.

Contents

Safety Cases

Projects, Services and Systems of Systems

Systems Safety in Healthcare

Testing Safety-Critical Systems

Technological Matters

Safety Standards