Achieving Systems Safety

Related Titles

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

Advances in Systems Safety
Proceedings of the Nineteenth Safety-Critical Systems Symposium, Southampton, UK, 2011
Dale and Anderson (Eds)
978-0-85729-132-5

Chris Dale • Tom Anderson
Editors

Achieving Systems Safety

Proceedings of the Twentieth Safety-Critical Systems Symposium, Bristol, UK, 7-9th February 2012

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

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

ISBN 978-1-4471-2493-1 e-ISBN 978-1-4471-2494-8
DOI 10.1007/978-1-4471-2494-8
Springer London Dordrecht Heidelberg New York

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

Library of Congress Control Number: 2011944278

The use of registered names, trademarks, etc., in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Printed on acid-free paper

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

Preface

This proceedings volume contains papers presented at the twentieth Safety-critical Systems Symposium (SSS 2012). 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; we are grateful to them for their contributions.

In his opening keynote address, Martyn Thomas highlights vulnerabilities in GPS and other global navigation satellite systems, thus illustrating that many general purpose systems can have an impact on safety. The two following papers address the importance of culture and community to the achievement of safety.

Roger Rivett's keynote paper looks at the challenge of technological change in the automotive industry. This is followed by three other papers on transport safety: one focuses on unmanned aerial systems, and the other two on railways.

Cyber-attacks on safety-critical systems form the subject of Chris Johnson's keynote talk. Four papers then look at improving our approach to systems safety: taking account of electromagnetic interference; treating safety as a viewpoint on systems engineering; safety architectural patterns; and Bayesian belief networks.

Next, two papers look at accidents: how should we investigate them and what can we learn thereby. The second of these is Peter Ladkin's keynote on the accident to the nuclear reactors at Fukushima.

Jens Braband's keynote paper presents a risk-based approach to assessing potential safety deficiencies. This is followed by two papers on validating safety-critical software, and on software testing.

The final keynote, by John McDermid and Andrew Rae, focuses on goal-based safety standards, and is followed by two papers that look in detail at safety levels.

We are grateful to our sponsors for their valuable support and to 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 2011

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.
- 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

Keynote Address

Accidental Systems, Hidden Assumptions and Safety Assurance
Martyn Thomas 1

Do we truly understand Safety Culture?
Allan Bain 11

The Need for a Community for System and Functional Safety Professionals
Audrey Canning 25

Keynote Address

The Challenge of Technological Change in the Automotive Industry
Roger Rivett 35

Safety Process Implementation for Unmanned Aerial Systems
Sirma Celik 43

Risk Analysis and Development of an IP-Network-based Railway Signal Control System
Reiji Ishima and Minoru Mori 55

Taking Safe Decisions in the GB Railway Industry
George Bearfield 75

Keynote Address

CyberSafety: CyberSecurity and Safety-Critical Software Engineering
Chris Johnson 85

Including Electromagnetic Interference (EMI) in Functional Safety Risk Assessments
Keith Armstrong 97

Safety Engineering – a Perspective on Systems Engineering
Derek Fowler and Ronald Pierce 115

Survey of Safety Architectural Patterns
Paul Hampton 137

The Application of Bayesian Belief Networks to Assurance Case Preparation
Chris Hobbs and Martin Lloyd 159

Accident Investigation – are we reaching the Systemic Causes of Accidents?
Graham Braithwaite 177

Keynote Address
The Fukushima Accident
Peter Ladkin 189

Keynote Address
A Risk-based Approach towards Assessment of Potential Safety Deficiencies
Jens Braband 209

At the Sharp End: developing and validating Safety Critical Software
Fergus Duncan 225

The New Software Testing Standard
Stuart Reid 237

Keynote Address
Goal-Based Safety Standards: Promises and Pitfalls
John McDermid and Andrew Rae 257

Safety Levels in a Commercial Context
Mike Parsons 271

A Devil's Advocate on SIL 4
Odd Nordland 285

Author Index 293