

Improvements in System Safety

Related titles:

Towards System Safety

Proceedings of the Seventh Safety-critical Systems Symposium, Huntingdon, UK, 1999

Redmill and Anderson (Eds)

1-85233-064-3

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

Felix Redmill Tom Anderson
Editors

Improvements in System Safety

Proceedings of the Sixteenth Safety-critical Systems
Symposium, Bristol, UK, 5–7 February 2008

**Safety-Critical
Systems Club**

BAE SYSTEMS

 Springer

Felix Redmill
Redmill Consultancy
22 Onslow Gardens
London N10 3JU
UK

Tom Anderson
Centre for Software Reliability
University of Newcastle
Newcastle upon Tyne, NE1 7RU
UK

ISBN: 978-1-84800-099-5 e-ISBN: 978-1-84800-100-8
DOI 10.1007/978-1-84800-100-8

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

© Springer-Verlag London Limited 2008

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

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

9 8 7 6 5 4 3 2 1

Springer Science+Business Media
springer.com

Preface

The Safety-critical Systems Symposium (SSS), held each February for sixteen 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 '08.

The first paper accompanies the tutorial, which is on the important topic of the safety case. In recent years, the emphasis of papers has shifted from defining and describing the safety case and its purposes to reporting on experiences of its use and developments in its theory. Two further papers in the book do this.

The Symposium is for engineers, managers, and academics in the field of safety, across all industry sectors, so its papers always cover a range of topics. Each year a number of papers address themes raised in the previous year, and the papers in the section on the safety case are examples of this. In addition, there is a section of individual papers, on the relationship between safety and security, safety process improvement, and software development.

Over the years, there has been increasing emphasis on the role of humans, not only in contributing to accidents but also in achieving safety. Thus, 'human factors' is a recurring topic at the Symposium. And the need to develop and maintain a good safety culture has also come to be recognised as an important topic. This year there are papers on both subjects.

In the final two sections, a number of papers address the key subjects of risk analysis and the achievement and assessment of overall safety. These topics are perennial, for they require both good process and methodical technique, and every year there are papers that make observations, present reports on informative experiences, and offer new ideas. This year is no exception, and the five papers in the two sections do all of these things.

Overall, the papers address many of the topics that are currently of special interest in the safety-critical-systems community, and we are grateful to the authors 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 with their planning and organisation.

FR & TA
October 2007

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 at the Centre for Software Reliability (CSR) in the University of Newcastle upon Tyne, and its Co-ordinator is Felix Redmill of Redmill Consultancy.

Since 1994 the Club has been self-sufficient, but it retains the active support of the DTI and EPSRC, as well as that of the Health and Safety Executive, the Institution of Engineering and Technology, and the British Computer Society. 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 1- and 2-day seminars each year;
- Providing tutorials on relevant subjects;
- Publishing a newsletter, Safety Systems, three times annually (since 1991), in January, May and September.

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, and these can be paid at the first meeting attended.

To join, please contact Mrs Joan Atkinson at: The Centre for Software Reliability, University of Newcastle upon Tyne, NE1 7RU; Telephone: 0191 221 2222; Fax: 0191 222 7995; Email: csr@newcastle.ac.uk

Contents List

Tutorial Paper

Can Process-Based and Product-Based Approaches to Software Safety Certification be Reconciled?

Tim Kelly 3

Themes Reprised from SSS '07

Making Safe Software Secure

Odd Nordland 15

Safety Process Improvement with POSE and Alloy

Derek Mannering, Jon Hall and Lucia Rapanotti..... 25

How to Select a Programming Language Subset to Maximise Software Quality

Wojciech Basalaj..... 43

The Safety Case

Safety Case Development – How can I continue the work?

Tadeusz Cichocki..... 59

Safety Case Experiences from Harrier

Jeff Lucas 77

Safety Culture

Investigation to Establish Whether Cultural Analysis Can Be Used to Improve the Interactions Between Design, Safety and Operations Departments

Tim Smith 95

Human Performance Improvement – Reducing Significant Events in Nuclear Power

Don Goble..... 117

Human Factors

A Human Factors Perspective on Safety Management Systems

Christopher Lowe..... 139

Human Factors Safety Assurance for Changing ATM Systems

Stephen Clark, Steven Shorrock and Nic Turley 155

Achieving and Improving System Safety

Practical Ways of Improving Product Safety in Industry <i>Gabriele Schedl and Werner Winkelbauer</i>	177
Prototyping versus Formal Development <i>Mike Ainsworth</i>	195
Systems Approach to Unmanned Air Vehicle Development and Certification <i>Richard Sleeman, Andrew Cox and Jenny Colledge</i>	209

Safety and Risk Analysis

Safety Analysis: Thoughts on Methods and Experience <i>Michael Ellims</i>	225
Simplifying the Creation and Use of the Risk Matrix <i>Robin Cook</i>	239
Author Index	265