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

Felix Redmill and Tom Anderson (Eds)

The Safety of Systems

Proceedings of the Fifteenth Safety-critical Systems Symposium, Bristol, UK, 13-15 February 2007

Safety-Critical Systems Club

BAE SYSTEMS

Springer

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

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

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

ISBN-10: 1-84628-805-3 Printed on acid-free paper
ISBN-13: 978-1-84628-805-0

9 8 7 6 5 4 3 2 1

Springer Science+Business Media
springer.com

PREFACE

Since 1993 the Safety-Critical Systems Club has hosted the Safety-critical Systems Symposium (SSS) each February. Every year the programme has reflected what is then of particular interest to the safety community – in ways of working, in analysis techniques, in technology, in standards, and in research work that is on the point of being useful to practitioners. This book presents the papers delivered at the landmark fifteenth SSS.

A subject that is mostly neglected by safety practitioners but which, if studied more carefully, could lead to both technical and economic efficiencies, as well as more effective protection, is the relationship between safety and security. The management of both is based on risk analysis and there are indications that the analyses could effectively be combined. The Symposium has offered papers on this subject in the past, and this year there are three.

Continuing the trend of recent years, there are five papers on the development of safety cases, which are intended to demonstrate, or claim, the achievement of safety – in defined applications and under given circumstances. Some of the papers report on experiences in the field, but others venture to propose new ways in which safety cases may be used or extended.

Other areas of the safety domain whose importance is increasingly being recognised are safety management and safety assessment, and both are represented by three-paper sessions. One of the assessment papers is on human reliability assessment, a topic with which engineers are advised to familiarise themselves to a greater extent than hitherto. Indeed, a useful starting point is this paper, for it offers some historic background as well as a review of the techniques in the field.

The final section at the Symposium, and of this book, is on the use of 'formal' methods in achieving and demonstrating safety. Such methods have in the past been deemed to be expensive and only worth using in extreme circumstances, but many now claim that their proper use achieves such advantages that they should be employed as a matter of course. The papers here are on specification and the C language.

Whereas this book represents the content of the Symposium, it can only hint at the effort that goes into the event's organisation. We thank the papers' authors and their organisations for writing and presenting their papers and, thus, for contributing to a substantial Proceedings. We also thank Joan Atkinson for her continued indefatigable efforts in arranging the event's logistics, upon which everything else depends. And we look forward to SSS '08, planning for which has already commenced.

FR & TA
November 2006

THE SAFETY-CRITICAL SYSTEMS CLUB
organiser of the
Safety-critical Systems Symposium

What is the Club?
The Safety-Critical Systems Club exists 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. It is an independent, non-profit organisation that co-operates with all bodies involved with safety-critical systems.

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 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 safety engineering and management and provides a forum for experienced practitioners to meet each other and for the exposure of newcomers to the safety-critical systems industry.

Focus of 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. Without sponsorship, the Club depends on members' subscriptions, which can be paid at the first meeting attended.

To join, please contact Mrs Joan Atkinson at: 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

Trends in Safety Case Development

Lessons in Safety Assessment

High Integrity from Specification to Code