Constituents of Modern System-safety Thinking

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

Felix Redmill and Tom Anderson (Eds)

Constituents of Modern System-safety Thinking

Proceedings of the Thirteenth Safety-critical Systems Symposium, Southampton, UK, 8-10 February 2005

Safety-Critical Systems Club

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

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.

ISBN 1-85233-952-7
Springer Science+Business Media
springeronline.com

© Springer-Verlag London Limited 2005
Printed in Great Britain

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.

Typesetting: Camera ready by contributors
Printed and bound by the Athenæum Press Ltd., Gateshead, Tyne & Wear
34/3830-543210 Printed on acid-free paper SPIN 11316947

PREFACE

The papers in this book address topics that are of crucial importance in current safety thinking. The core of modern safety thinking and practice is a risk-based approach, and, not only is this a 'given' in all of the papers, but also one session of two papers is devoted to an exploration of the subject of risk. Another fundamental of safety engineering and management is the need not merely to achieve safety but to demonstrate its achievement in advance of deploying a system. This requires the construction of an argument (a safety case) that the system is adequately safe for its intended application, and the independent safety assessment of the argument. Both of these topics – the safety case and safety assessment – are addressed in papers in this volume. Indeed, they are recurring themes at the annual Safety-critical Systems Symposium, for both are in the process of development and change.

Another topic reprised in this book is accident investigation, for, whenever an investigation takes place, lessons are learned not only about the accident itself but also about the investigation process. Two papers in this book make strong contributions in this field. Then, there is the issue of commonality between the processes and techniques employed in safety and security engineering. Typically, the one discipline looks outwards and the other inwards, but they both take a risk-based approach and both employ techniques to identify and analyse the risks and processes to manage them. Yet there is little attempt by the two communities to come together, compare notes, and learn from each other. This Symposium has in the past invited papers that prompt such communication, and, again, this year's event points to similarities between the two disciplines and an inherent interdependence between them.

But the major themes are not mutually exclusive. Through them run common threads, including 'blueprints' for specification and definition, the use and development of technology, and the human factor. Safety is multi-dimensional, in both concept and practice.

On behalf of the Safety-Critical Systems Club, the promoter of the Symposium, we gratefully thank the authors for their contributions to the event and this book. And for the thirteenth successive year, we thank Joan Atkinson who so ably manages the Club's secretariat and organises the event's logistics.

FR & TA
November 2004

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 and to facilitate technology transfer in the field of safety-critical systems. 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 had to be 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 Electrical Engineers, and the British Computer Society. All of these bodies are represented on the Club's Steering Group.

What does the Club do?

The Club achieves its goals of technology transfer and awareness-raising 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 each year (since 1991), in January, May and September.

How does the Club help?

The Club brings together technical and managerial personnel within all sectors of the safety-critical community. It provides education and training

in principles and techniques, and facilitates the dispersion 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.

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 a 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

INDEPENDENT SAFETY ASSESSMENT

The IEE/BCS Independent Safety Assurance Working Group
David H Smith 3

Putting Trust into Safety Arguments
Jane Fenn and Brian Jepson 21

Independent Safety Assessment of Safety Arguments
Peter Froome 37

SAFETY AND SECURITY

Structuring a Safety Case for an Air Traffic Control Operations Room
Ron Pierce and Herman Baret 51

SafSec: Commonalities Between Safety and Security Assurance
Samantha Lautieri, David Cooper and David Jackson 65

ACCIDENT INVESTIGATION

Learning from a Train Derailment
Kevin Payne 79

Accident Investigations – Meeting the Challenge of New Technology
Knut Rygh 93

RISK AND ITS TOLERABILITY

Identification of Time At Risk Periods of Significance to ALARP Justifications
Mark George 111

Developing and Using Risk Matrices
Michael Prince 129

ACHIEVING AND ARGUING THE SAFETY OF MODULAR SYSTEMS

Health Monitoring for Reconfigurable Integrated Control Systems
Mark Nicholson 149

Exploring the Possibilities Towards a Preliminary Safety Case for IMA Blueprints
Graham Jolliffe and Mark Nicholson 163

Modular Certification of Integrated Modular Systems
James Blow, Andrew Cox and Paul Liddell 183

TECHNOLOGIES FOR DEPENDABILITY

The Effects of Timing and Collaboration on Dependability in the Neonatal Intensive Care Unit
Gordon D Baxter, Juliana Küster Filipe, Angela Miguel and Kenneth Tan 195

Applying Java Technologies to Mission-Critical and Safety-Critical Development
Kelvin Nilsen and Adrian Larkham 211