

Advances

in Safety Critical Systems

*Results and Achievements from the DTI/EPSRC
R&D Programme
in Safety Critical Systems*

Compiled and Edited by Mike Falla
JUNE 1997

Contents

Preface *see below*

1 Introduction

- 1.1 The Safety Critical Systems Programme
- 1.2 Purpose and structure of this book

2 Are your systems critical?

- 2.1 Legal liability for defective systems
- 2.2 Emerging software safety standards
- 2.3 IEC 1508

3 Hazard Analysis

- 3.1 Software hazard analysis
- 3.2 Integrating software hazard analysis with the development process
- 3.3 HAZOP throughout the lifecycle
- 3.4 A case study of Fault Tree Analysis
- 3.5 Mobile robots
- 3.6 A method for hazard assessment in programmable systems

4 Making the Case that it's Safe

- 4.1 A method for safety cases
- 4.2 A designer's assistant
- 4.3 Combining diverse evidence

5 Assessment

- 5.1 A Framework for Assessment
- 5.2 Guidelines for assessment

6 Managing Risk and Safety

- 6.1 Managing risk
- 6.2 Safety policies and models

7 The Interface with the Operator

- 7.1 Supporting team operation
- 7.2 Analysing human error
- 7.3 Hazard analysis of human interaction

8 Guidelines for Best Practice

- 8.1 Automotive industry
- 8.2 Management guidelines for developing safety-critical software
- 8.3 A methodology for safe advanced robots
- 8.4 A code of practice for the human dimension
- 8.5 Guidelines for programmable logic controllers

9 Getting the Process Right

- 9.1 The safety-critical systems engineering process
- 9.2 The problem of changing requirements
- 9.3 The legal lifecycle
- 9.4 Modelling the process using AI techniques
- 9.5 Communication in engineering design

10 Tools and Languages for Critical Systems

- 10.1 Tools for railway signalling
- 10.2 Reverse engineering safety-critical systems
- 10.3 Design patterns and frameworks
- 10.4 Assessing the impact of object technology in the safety-critical domain.

11 The Human Element in the Development Process

- 11.1 Predicting fault rates during software development
- 11.2 Avoiding human error in design
- 11.3 A systems approach to human error
- 11.4 Designers' practices

12 Testing

- 12.1 Environment simulation
- 12.2 The contribution of testing to safety cases
- 12.3 Case studies
- 12.4 How much testing do I need to do?
- 12.5 Measuring the testability of a system

13 Formal Methods

- 13.1 Formal Methods for cost-effective procurement of high integrity systems
- 13.2 Case studies with RAISE in avionics, plant control and laboratory information
- 13.3 Reverse engineering by formal transformations

14 New Approaches to Critical Systems

- 14.1 Knowledge-based systems and safety-critical decisions
- 14.2 Functional programming languages for complex systems
- 14.3 Neural computing
- 14.4 Using natural language processing tools

15 System Architectures

- 15.1 Supporting re-use
- 15.2 An architecture for mobile robots
- 15.3 The multiversion approach to ultra-reliability

16 Safety-Related Engineering Design

- 16.1 Safe structural analysis
- 16.2 Safe design of networks

Appendices

- A The Projects
- B The Genesis of the Programme
- C The Organisations Involved
- D Acknowledgements

Preface

It is now a little over ten years since a group of us representing government departments and the professional institutions gathered at the headquarters of the UK Health and Safety Executive. We were trying to decide what action we might take given a growing concern in the trade press and among professionals about the way in which we were managing the development of safety-critical computer-based systems.

At that time there was much misunderstanding. We all came from different industry sectors, with different traditions, different regulatory requirements, different standards, and different ways of managing computing technology in critical applications.

It is clear from the sheer diversity of work reported in this book that there are still many differences. Moreover, technology and the market have both developed dramatically during those ten years, complicating the picture still further. But over that time we have built a community with at least a better mutual understanding.

In particular we have recognised that there are no simple solutions: but we have generally agreed strategies such as those embodied in the IEC 1508 Standard, in the general principle of the safety case, and in the evolving form of a safety case. These give us a framework for incorporation of more knowledge as we acquire it. There is certainly much more to be learned.

The next challenge is to find ways to encapsulate some of our understanding for others who are not part of this research community but are simply building systems - increasingly, safety critical systems. Telling them the big lesson that we have learned - that the problem is more difficult than we had appreciated - does not help them a lot.

There are many to thank for their support and patience during the work reported here, apart from the researchers themselves. There are the professional institutions, the individuals who gave their time and their employers, and, of course, the DTI and the EPSRC who, with industry, funded the programme which supported much of the work.

I would finally like to thank Mike Falla for his diligence in making such a coherent presentation of the work reported here. As co-ordinator for the programme, I have often said that my ambition was to engender greater mutual understanding through comparison and contrast of a broad range of technologies, applications, and industrial environments. I claim to have done the easy bit - to create the contrasts. Mike has done the more difficult bit - the considered comparison of these ideas and activities.

Bob Malcolm