Preface

Computer-based systems are now essential to everyday life. They involve both technical (hardware/software) components and human beings as active participants. Whenever we fly aboard an aircraft or withdraw money from a cash point, a combination of humans, machines and software is supporting the delivery of the service. These systems and many others benefit from the miniaturisation and cost reduction of the hardware which has made it possible for computers to be embedded everywhere. An equally remarkable development is the software involved: today, systems are built which were literally unthinkable twenty or thirty years ago. Measured in terms of their function, the productivity of their creation has also advanced enormously (largely because of the software infrastructure). Even the dependability of the best of todays software is praiseworthy when one considers the complexity of the functionality provided. Solid engineering and the increasing adoption of methods based on firmly established theory are to be thanked here. However, in large and complex systems, there remain major challenges to achieving dependability when complex interactions exist between technical and human components.

Large and complex things are understood as assemblages of simpler components: the way these components fit together is the *structure* of the system. Structure can be real and physical, or a subjective mental tool for analysis. It is often possible to view a complex system as having different structures: one useful view of the eventual structure will often be strongly related to the way in which the system was built (or came into being). This book addresses many aspects of the way in which structure can affect the dependability of computer-based systems. It is, for example, essential to be able to identify checking and recovery components and layers in the structure of a system; it is equally important to be able to analyse the dependability of a complex system in terms of the dependability of its components and of the way those components can affect each other within the system structure.

The work on the connection of structure with dependability of systems is one outcome of a large interdisciplinary project, DIRC[1], which started in 2000. The DIRC researchers come from a number of disciplines including computing science, psychol-

[1]The Dependability Interdisciplinary Research Collaboration: visit DIRC at http://www.dirc.org.uk

ogy, sociology and statistics. Within this project, funded by EPSRC[2], it is assumed that computer-based systems are multi-faceted in such a way that their design and analysis (in the largest sense) require skills that reach far beyond the computational and informatics aspects of the problem. To guarantee delivery of an acceptable service many dimensions must be taken into account – for instance, how humans use computers, security concerns, and the sociological implications of integrating machines into a pre-existing environment. All of these dimensions have structural aspects. The diverse set of researchers engaged over five years in the DIRC collaboration offers a unique opportunity for an interdisciplinary book on this fundamental topic of structure, drawing on a broad range of contributions. We hope that it will provide practitioners, commissioners and researchers with an important resource.

The two introductory chapters (by Jones & Randell, and Jackson, respectively) provide complementary visions. Jones and Randell discuss a well-known analysis framework (the dependability taxonomy) that categorises both problems and their mitigation. This framework defines a number of terms that readers will encounter throughout the book. In contrast to this theoretical view of computer-based systems, Jackson demonstrates that software engineering requires a decompositional analysis of a problem.

In the *System properties* section, Felici describes a central feature of systems: evolution. He puts forward the idea that there is not just one evolution, but several in parallel, ranging from a piece of software to the entire organisation, that together define the life of the computer-based system. The second contribution to the *System properties* section deals with time. Burns and Baxter develop Newells theory of time bands and demonstrate how this framework can help to analyse time-related events at a variety of granularities within computer-based systems.

The *Human components* section specifically adopts a human-centred view of systems. Besnard focuses on how dependability can be enhanced or hindered by the application of rules. The application of procedures and programs by the corresponding agent (human or machine) is addressed by considering a number of industrial cases. An industrial case-based approach also drives the chapter from Besnard and Baxter in their analysis of cognitive conflicts. They demonstrate how important it is that humans interacting with an automated system should understand the principles of its functioning.

To specify which features a given system should have, one must be able to understand what the system is doing, whatever its scale. This is the scope of the *System descriptions* section. In this section, the authors discuss examples of description techniques at four different granularities. The first level is software-based. Gacek and de Lemos discuss architectural description languages (ADLs) for capturing and analysing the architecture of software systems and how they can help in achieving dependability. The second level of granularity is about reasoning and visualising problems. Gurr describes how diagrams can be used to convey an intuitive understanding of complex logical relations between abstract objects. The third level of granularity is ethnographic: Martin and Sommerville discuss the relationship between the social structure of work and the technical structure of a system. They emphasise the importance of un-

[2]EPRSC is the UK Engineering and Physical Sciences Research Council: visit EPSRC at http://www.epsrc.org.uk

derstanding this relationship when designing dependable socio-technical systems. The fourth and last level is organisational: Andras and Charlton use abstract communications systems theory to demonstrate that the various adaptations and failure modes of organisations can be described in terms of the communications exchanged.

Guaranteeing dependability is the fifth and final section of the book. It deals in a practical manner with the task of ensuring that dependability is achieved – or understanding why it might not be achieved. Bryans and Arief address the topic of security. They adopt a human perspective on computer-based systems. Security is too often regarded as a purely technical issue, thereby leaving unprotected paths in the surrounding human system to be exploited by malicious attacks. Jackson tackles system weaknesses from an engineering point of view. In his approach, system failures are partly due to the way software engineers capture requirements. An intellectual structure for software development is proposed and discussed on the basis of a concrete example. But certifying that a system will behave dependably is also related to information gained *after* it is developed. Bloomfield and Littlewood consider critical systems certification. On the basis of a statistical analysis, they address the question "What happens when you want to certify a system and must combine arguments drawing on different statistical information"? The question of arguments is also addressed by Sujan, Smith and Harrison, who investigate the choice and combination of arguments in dependability claims.

This book could have been much longer and covered yet more topics. But it was never the goal to provide an exhaustive view of the structure of computer-based systems. Rather, the driving force was a desire to shed light on some issues that we considered particularly important. The editors hope that by bringing together varied topics with a common theme they have provided readers with a feel for the importance of interdisciplinarity in the design, commissioning and analysis of computer-based systems. Inevitably, practice changes only slowly. But we hope we have been able to offer a wider vision, showing how seemingly distinct concerns are sometimes closely interwoven, and revealing to practitioners of one discipline the relevance and importance of the problems addressed by another. Customers, stakeholders and users of computer-based systems may also benefit from an understanding of the underlying connections among different facets of their system.

The authors themselves have benefited from writing this book: it gave an increased opportunity to cross the boundaries of our disciplines and share views with researchers from different backgrounds. We are now more than ever convinced of the value of different perspectives derived from different backgrounds: this is where the importance of interdisciplinarity lies. We also hope that this book, beyond any direct influence of its contents, will disseminate a certain philosophy of undertaking science in the field of dependability. After all, through the knowledge it builds, the work done in dependability has a mission of contributing to the construction of our society's future. How could this be better achieved than through knowledge sharing and integration?

Acknowledgements:

Individual authors wish to express acknowledgements as follows

Burns and Baxter: The time band formulation owes much to the input of Colin Fidge and Ian Hayes. This particular description has benefited from comments of Denis Besnard and Cliff Jones.

Besnard: The author is grateful to Cliff Jones for his initial effort on Chapter 5 and his continuous help. Brian Randell, Gordon Baxter and Andrew Monk should also be thanked for their very constructive comments on earlier versions of this text.

Jackson: Talking and working with colleagues in the DIRC project and at the Open University has greatly helped my understanding of the matters discussed in Chapter 12. The irrigation problem has been extensively discussed with Cliff Jones and Ian Hayes, and is the subject of a jointly authored paper. I am grateful to Tom Maibaum for introducing me to Walter Vincenti's illuminating book. Cliff Jones, Ian Hayes and Denis Besnard read an earlier draft of this chapter and made many valuable comments.

Bloomfield and Littlewood: The work discussed in Chapter 13 was partially supported by the DISPO-2 (DIverse Software PrOject) Project, funded by British Energy Generation Ltd and BNFL Magnox Generation under the IMC (Industry Management Committee) Nuclear Research Programme under Contract No. PP/40030532. An earlier version of this paper was presented at the International Conference on Dependable Systems and Networks (DSN2003) in San Francisco.

Sujan, Smith and Harrison: Are grateful to Lorenzo Strigini and Michael Hildebrand for insightful comments and discussions.

As a closing word, we emphasise that the idea of dependability as an interdisciplinary scientific domain – an idea that underlies the variety of the chapters of this volume – rests firmly on the work of the authors. They provided the material for our message; they invested their time and expertise in the achievement of this book and should be thanked warmly. Behind the scenes lies a partner that made this collaboration possible: EPSRC. The Research Council made the gathering of the interdisciplinary team possible and thus provided the essential conditions for this book to be written. All of the authors and editors are grateful to EPSRC for the funding of DIRC ('Interdisciplinary Research Collaboration in Dependability of Computer-Based Systems').

The editors would also like to thank sincerely their long-suffering "production team" Joanne Allison and Joey Coleman without whom the chapters would probably have never made it into a book – certainly not one so well presented as this. Thanks are also due to our publisher Springer.

Denis Besnard
Cristina Gacek
Cliff B Jones
Newcastle upon Tyne, July 2005

http://www.springer.com/978-1-84628-110-5

Structure for Dependability: Computer-Based Systems from an Interdisciplinary Perspective

Besnard, D.; Gacek, C.; Jones, C.

2006, XII, 306 p. 50 illus., Softcover
ISBN: 978-1-84628-110-5