

DIRC: an interdisciplinary attack on problems of Dependability

D Greathead and C B Jones

University of Newcastle upon Tyne
Newcastle, NE1 7RU, UK
cliff.jones@ncl.ac.uk

Abstract. DIRC is a large, six year, project funded by the UK research council EPSRC. Outlined here are some insights into the research themes around which DIRC's work is structured, some of the collaborations with our industrial partners and our plans for the future.

1 Introduction

The Dependability Interdisciplinary Collaboration (DIRC) is a six year project with five UK University partners: Newcastle upon Tyne (the lead site), City, Edinburgh, Lancaster and York. Researchers come from multiple disciplines: computer science, psychology, sociology and statistics. An *Industrial Advisory Board* helps to ensure that the project's research addresses issues that are relevant to computer-based systems in many application areas. The Board draws members from organisations as diverse as Barclays, Philips Medical Systems, Microsoft Research, QinetiQ, Adelar, Dependable Systems, National Air Traffic Services (NATS), Praxis Critical Systems and Voca.

1.1 The context for DIRC

As computers have become faster and cheaper they have become embedded in our lives to such an extent that we barely notice them unless something fails. The more we demand of them, the more complex computer-based systems become — but they must remain dependable: reliable, safe and secure.

DIRC uses the term *computer-based system* to mean one in which hardware, software and people combine. In these broad socio-technical systems, researchers must consider the interactions between computer systems and their users. They must understand how people and organisations cope with failures and unexpected events. Dependable systems should not only minimise the risk of hardware and software failures, they must also reduce the risk of failures resulting from users' actions. They must provide support for users to help them cope with, and recover from, system problems. Outside the technical system, organisational policies should also be designed for dependability.

1.2 An interdisciplinary approach

With such diverse elements in computer-based systems, an interdisciplinary approach is crucial if systems are to become more dependable. In DIRC, computer scientists, psychologists, sociologists and statisticians have integrated their research to the extent that DIRC's reviewers have characterised its work as "redefining the international scientific landscape for dependable systems research".

The first phase of DIRC's six-year programme focused on analysis of existing systems and the methods used to create them. This phase has also seen dependability ideas known to work for purely technical ("safety critical") systems developed to tackle computer-based systems. DIRC researchers have combined their disciplinary perspectives to carry out in-depth analyses of applications in areas such as the Health Service, manufacturing, energy, air traffic control and the use of computers to enable people to stay in their homes rather than having to move to a residential care environment. The understanding developed in this phase is informing the development of methods and tools to enable others to create computer-based systems with increased dependability.

Not only have we learned to recognise and respect the diverse values of the disciplines, we have also learned the value of tackling application problems together as a team. With an "Operations Research" (OR) like team drawn from several disciplines, terminology problems disappear, contributions become understood and something is achieved which no single discipline could have envisaged.

1.3 Moving forward

In the second phase, DIRC researchers are focusing on synthesising their findings into material that will inform future system designs. The knowledge and understanding gained by DIRC's researchers has led to collaborations with organisations such as NATS and Voca who rely on extremely complex systems and have dependability as a major priority.

2 The research themes

The synthesis of ideas is being documented around five Research Themes.

Structure Understanding a complex computer-based system means comprehending its structure and in designing a successful system the right structure is essential. DIRC has emphasised the issue of designing barriers to limit the propagation of failures. This idea is well known in technical systems but designers of wider computer-based systems need a deeper awareness of its benefits. Processes, for humans as well as machines, need to be understood as trying to keep a system in a "desired envelope" of operation or returning the system to the desired state in the event of a deviation.

Planning for *evolution* of requirements is another key issue for structure: most systems evolve as needs change; *all* computer-based systems evolve precisely because humans are involved.

Risk Human perception of risk is often at variance with the technical analysis of the risk of system failure: driving your own car carries higher risks than travelling by train and yet reducing the risk of rail accidents attracts more resource than road safety measures. The perception of risk by the people who are part of a computer-based system is clearly important in terms of the system deployment and DIRC is applying work done in the social sciences to these systems.

Dependability cases do not consider only the reliability of a system, they must also consider the level of confidence with which that reliability is predicted. DIRC is breaking new ground in assessing the degree of confidence that might be placed in a complex computer-based system prior to its deployment by analysing risk from many perspectives including organisational, cultural, technological, structural and psychological.

Diversity The use of diversity to make things dependable is something we understand intuitively: don't put all your eggs in one basket. Related to such simple, everyday notions are sophisticated engineering ideas, such as the use of multiple independent programming teams to create multi-version software in mission critical applications.

Replicating things that might exhibit the same failure modes is pointless; DIRC is investigating the use of diversity to achieve dependability. For example, in an empirical study of the impact of a computer system designed to help in medical image analysis, the diversity viewpoint provides important new insight about the effectiveness of the tool in reducing errors and whether some errors might even result from its deployment.

Responsibility Confusion over responsibility is a common cause of system failure. For example, Alice may fail to take some action because she thinks Bob is responsible whereas Bob believes that it is Alice's responsibility. Such problems can arise because responsibilities are not well defined, are often implicitly assigned and delegated and may be interpreted differently.

Building dependable systems requires an understanding of the notions of responsibility held by the practitioners who will use the system — for instance, who can view or update information and for what purpose. DIRC is seeking ways to make responsibilities explicit in models that can be used to inform system design, providing a basis for reasoning about responsibilities and allowing identification of areas of critical conflict or vulnerability in a computer-based system.

Timeliness A single computer-based system may have to accommodate actions at very different timescales: from a critical calculation carried out within microseconds to an alarm that allows a human operator adequate time to respond to a malfunction. Understanding the potential tensions and conflicts is key to designing dependable systems.

In modelling schemes and informal descriptions, the representation of time is often over-simplified. Such a representation limits understanding of the structural properties of the system; it also fails to support the separation of concerns that can come from thinking about the different time

scales of the system. DIRC is making a real contribution to system analysis methods by emphasising how increased understanding of time bands can lead to better comprehension of complex computer-based systems.

3 Some outcomes

It is an important measure of success for DIRC that the development of computer-based systems in a variety of application areas is being influenced by the work of the project. Some of the projects achievements include:

- Donald MacKenzie’s prize winning book, others by Keith Stenning, Luciana D’Adderio and (editors) Karen Clarke and Gillian Hardstone are published or in the final stages of production.
- Work by Hardstone and Anderson has identified classifications as crucial “interface objects”. This role for classifications is particularly clear in the medical world where what is ostensibly a medical taxonomy is also used for accounting purposes.
- DIRC has developed a definition of “virtual organisations” or “dynamic coalitions”. These terms are used increasingly and DIRCs work will enable the study of information flow for the partners involved in such coalitions.
- Where much ethnographic research requires that a system is in place before sociologists can study it, DIRCs work on “patterns of ethnography” uses a technique of grouping varieties of settings to transfer lessons across contexts.
- Taking into consideration both security and socio-technical issues, DIRCs study of electronic voting has led to enhanced and extended systems.
- Many claims are made for open source software, including enhanced dependability. Our findings suggest that it is a phrase that is widely used but rarely defined. Impressed by the work which led to the paper *The Many Meanings of Open Source*, our reviewers encouraged us to continue work on this topic.

More details of the project’s work and references to papers and books are available from www.dirc.org.uk or by e-mailing dirc-enquiries@ncl.ac.uk You can also download many of our papers from our website.

Acknowledgments

Our research acknowledgment is to the many colleagues involved in DIRC. We are all grateful to EPSRC for the six year funding window which we feel was essential to foster such a wide interdisciplinary span.