Challenges and Directions for Dependable Computing: Some Reflections

Brian Randell
any analysis of the challenges and directions for dependable computing, to be useful, must take into account the likely future.

three Laws which are certain to help shape this future are:

- Moore: “The number of transistors per chip will double every eighteen months” - this law has enabled the growth of the internet
- Metcalfe: "The usefulness of a network varies as the square of the number of users” - this law has made the growth actually happen
- Murphy: “If anything can go wrong, it will” - this law has got to us where we are now
3M - A Vision of the Future, and an Antidote to Hubris

- e.g. concerning the Ambient Society, in which “everything is connected to everything”
- many of these connections will in fact be transient, many others will be unexpected and unwanted
- the whole population of inter-connected computers and computer-like devices will not be components of one defined system
- rather there will be a huge number of separately designed systems (by no means all carefully pre-specified and designed), but also systems-of-systems - both designed, and accidental
- many dependability problems will be caused by uncontrolled interactions, not necessarily via direct electronic links (and there will be infrastructure interdependencies!)
The Primacy of Socio-Technology

• each of the “3M laws” is socio-technological, not merely technological
• and most of the major systems we need to concern ourselves with are socio-technological, i.e. computer-based systems involving people as well as computers and networks (“non-electronic links”)
• moreover, many of these systems’ problems have socio-technological causes, whose solutions need to be grounded in (good) ‘socio-technology’.
The Wider World (1)

- public attitudes to dependability in general are confused and confusing
  - car accidents cause much less concern and attract much less publicity than plane crashes yet kill far more people - 40000 per annum!
  - dependability levels that are currently tolerated in desktop computers would not be acceptable in television sets
- what will public attitudes be to computer, and computer-caused, crashes in years to come?
The Wider World (2)

Economic and government pressures vary, and can have major impacts regarding system dependability:

- so-called “efficiency savings” can lead to fragile systems
- automation can reduce the frequency of minor failures, but in return for occasional much more costly failures
- previous balances that were held between individuals’ rights to privacy, and the state’s ability to monitor and control data communications have shifted abruptly since Sept 11
- some argue that development of a dependable global ICT infrastructure is being impeded by government and commercial policies, and that “open source” is the solution - is this still true, assuming it ever was?
The Wider World (3)

- software is a “natural monopoly” - (with very high development costs and virtually zero production costs, it is very difficult for new entrants to dislodge, or even co-exist alongside, a prominent market leader)
- thus in the PC world, competition is largely ineffective, e.g., in promoting dependability
- increasing software standardisation - e.g., on programming and user interfaces - presumably has a beneficial effect on the rate of at least certain types of accidental fault, as well as on development costs
- but lack of diversity contributes greatly to the impact of malicious faults
A Technical Agenda for Dependability R&D is Insufficient

- Simply listing a set of interesting technical challenges will not produce a defensible R&D programme:
  - socio-technical problems need socio-technical expertise
  - wider world issues have to be allowed for
  - projects must be chosen and conducted so as to maximise chances of take-up and industrialization, though not necessarily in the short term
  - a Dependability R&D Programme needs to be situated in its overall context (so its relation to, e.g. other IST programmes, is crucial)
  - the Dependability R&D Community needs also to use its expertise to benefit society in general

WG10.4, St. John, Jan. 2002
Some Possible Priority Topics

• the problems of subdividing responsibility (regarding functionality, error detection, and fault tolerance) between humans and computers in global computer-based systems
• intrusion-tolerant systems of (possibly mobile) systems - (in effect MAFTIA + DSoS++)!
• systems, and systems of systems, whose interfaces and specifications are ill-defined and/or evolving, yet need to be depended on continuously
• gaining a deeper understanding of such slippery concepts as “system complexity” (akin to recent work on “diversity”)
An Additional Dependability Research Challenge/Oportunity

- the GRID - a (very) well-funded global (socio-technological!) system, originated by the high energy physics community, initially advertised as a successor to the internet and the Web!
- first aimed at access to massive computing, like Arpanet was initially, now aimed at supporting “virtual organizations”
- Uses Linux plus Globus middleware
- IBM, Sun, etc., joining in (in part as a riposte to MS’s “.net”?)
- in US, little involvement of major CS departments, but in UK (and France?) they are becoming involved
- it raises major (short and long term) dependability issues

And for a UK view: http://e-science.ox.ac.uk/events/19-sep-2001/hey.htm

WG10.4, St. John, Jan. 2002
Two Obvious Points - Regarding Research Take-Up

• it easier to attract attention to a demonstratable mechanism, whether it be a system component, or a software tool that aids some aspect of the task of designing dependable systems, than to a technique that has to be taught and learnt.

• system components that can readily be integrated into existing systems have obvious advantages - (“reflection” is the modern successor to the “transparency” ideas we exploited with the Newcastle Connection 20 years ago)
Evidently, dependability researchers need to:

- take an active part in efforts aimed at enhancing public understanding of science,
- attempt to influence relevant government and commercial policy-forming activities, and
- encourage use of best current technical, and socio-technical practice.

The importance of “loop-closing” (à la de Bono), e.g.

- maintenance engineers flying in “repaired” planes
- system developers using their own systems