GC6: Dependable Systems Evolution

Report from the Grand Challenges Conference 2008:
Dr Juan Bicarregui
e-Science Information Services, e-Science Centre, Rutherford Appleton Laboratory; and member of GC6 Steering Committee

A long-standing computing challenge

We have 2,000 years of dependable systems evolution in civil engineering, for example in building bridges, but only 50 years in computer engineering.

Our grand challenge vision is of systems that are dependable and trustworthy throughout their lifespan.

The aim is to be able to prove that a program is correct before running it: this is an outstanding challenge in computer science that goes back 40 years.

The central principles are that theory should be embodied in tools, and tools should be tested against real systems.

Deliverables include a comprehensive theory of programming, covering the features needed to build practical and reliable programs; a coherent toolset automating the theory and scaling up; and a collection of examples.

Work is going on across the world, including in the UK, Europe, the USA, China and Brazil, on an international grand challenge in verified software. So part of the challenge is to ensure we can build on each others' work. Members of the steering committee have contributed to international development, workshops and conferences.

Targets, activities and progress

With much work going on in this area we are looking at a verified software repository, a managed repository of tools and challenges, to facilitate the use of tools and accelerate their development, and deepen knowledge of the challenges and progress development of design for analysis. Detail on the repository is at http://vsr.sourceforge.net/index.html and http://vsr.svn.sourceforge.net/viewvc/vsr/.

Each activity can accelerate the development of the other: tools development is encouraged and steered by challenges, and case studies are enhanced by results of analysis. From here we can provide feedback to tool developers and provide further analysis of the challenges. Meanwhile there can be constructive rivalry.

Since 2003 we have organised or contributed to more than 30 workshops, national and international conferences and other events.

We have run a project to verify a key property of the Mondex electronic purse on a smartcard, redoing work of 10 years ago. This was done by eight teams in different formalisms. The results from the teams were more or less the same - and all the results were much better than 10 years ago.

We also have a project in progress on specifying and verifying a flash memory filestore with fault tolerance. We have adopted a collaborative approach, with different teams doing different parts.

GC6 websites: http://vsr.sourceforge.net/introduction.htm http://www.fmnet.info/gc6/

Report from the Grand Challenges Conference 2004: http://www.ukcrc.org.uk/gcresearch.pdf

Report from the Grand Challenges Conference 2006: http://www.bcs.org/server.php?show=ConWebDoc.4721

Success criteria

How will we know when we have succeeded? Systems will be dependable: for example no blue screens from failed applications, no 404s (web page not found). Systems will have verified components, and verification will be invisible. Evolution will be exemplified by plug-and-play software with instant reconfiguration, interoperation and portability. And the development process will benefit from reduced testing, reduced test failures, and predictable development times and costs.