Safety by design

Analytical tools developed at the University of Oxford play vital roles in safety-critical and secure systems.

UNIVERSITY OF OXFORD

www.ox.ac.uk/oxfordimpacts

Computer systems that interact with each other are an increasingly common facet of everyday life. From safety-critical military applications to domestic uses like internet banking and e-commerce, it is vital that users have complete confidence in the functioning and security of the systems they are using.

Researchers from the University of Oxford's Department of Computer Science, directed by Professor Bill Roscoe, are developing complex tools that can check whether systems will really do what they promise. Their research builds on work by Professor Sir Tony Hoare, one of the world's foremost computer scientists, who was head of computer science at Oxford until 1999. Professor Hoare developed Communicating Sequential Processes (CSP), a formal mathematical language for describing the patterns of interaction between systems operating together, such as parallel processors, computers talking to each other, and the components of an individual microchip.

Professor Roscoe has pioneered Failures Divergence Refinement (FDR), a tool which analyses the interacting systems described in CSP and verifies mathematically that systems perform as they should. FDR has been used by QinetiQ (and its government-owned predecessors involved in defence research) in high-profile projects like the Eurofighter Typhoon aircraft and was also able to resolve a number of safety issues relating to defence technology.

The verification tool is now in use by universities and companies worldwide. Verum, a company set up by two graduates of the Department, now markets a commercial tool, ASD:Suite, for developing embedded software that allows developers to create right-first-time applications such as the 350,000 lines of code in the world's fastest digital pathology scanner (which makes and stores high-resolution digital images of tissue samples and biopsies), made by Philips Health Care. FDR is at the core of ASD:Suite.

Oxford researchers are now using FDR to develop secure interactions between mobile phones, bringing the prospect of secure information-sharing and mobile payment a step closer.

'Without CSP and FDR, what we do at Verum would be impossible, since there really are no alternatives! People who see what our tools do frequently express amazement that "theory" like CSP is being put to such practical use.'

Guy Broadfoot, Chief Technical Officer, Verum

www.cs.ox.ac.uk/ucs/CSPtools.html

Funded by: QinetiQ and Verum, the US Office of Naval Research, and the Engineering and Physical Sciences Research Council.