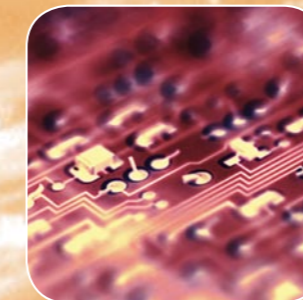
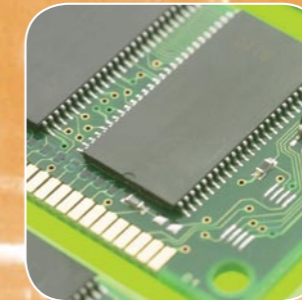
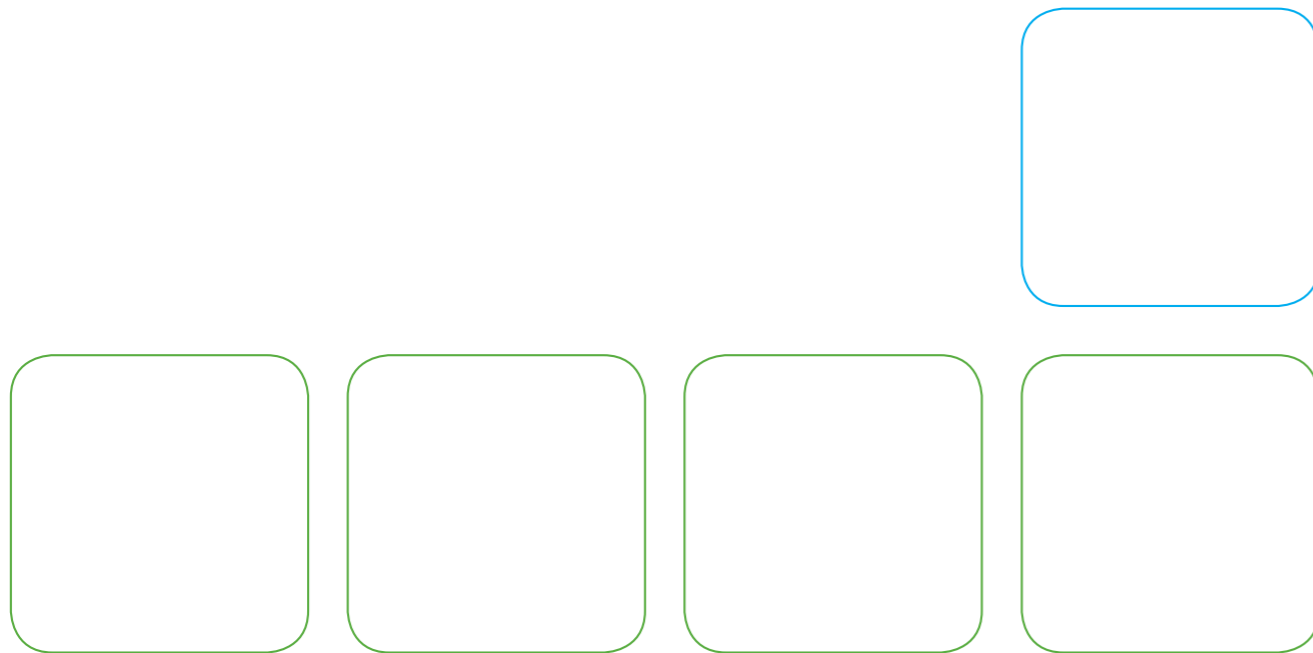


Contact Details

Prof. Gernot Heiser
NICTA – Neville Roach Laboratory
The University of NSW
Locked Bag 6016, NSW 1466
Telephone: +61 2 8306 0550
Facsimile: +61 2 8306 0406
Email: gernot.heiser@nicta.com.au
NICTA website: www.nicta.com.au



National ICT Australia is funded by the Australian Government's Department of Communications, Information Technology and the Arts and the Australian Research Council through Backing Australia's Ability and the ICT Centre of Excellence program.

NICTA is supported by its members:
• The Australian Capital Territory
• The Australian National University
• NSW Department of State and Regional Development
• The University of New South Wales

NICTA is supported by its affiliate partners:
• University of Sydney
• Victorian Government
• University of Melbourne
• Queensland Government
• Griffith University
• Queensland University of Technology
• The University of Queensland



Case study:
Improving the reliability of embedded computing systems

National ICT Australia

from imagination to impact...

2

The challenge

Rapid advances in hardware and software design are allowing significant computing power to be incorporated into an ever increasing number of devices.

Software programs that once needed large, expensive computer systems can now be run on a single processor chip. Indeed, the average mobile phone handset now contains computing capabilities comparable to those of a standard desktop PC of just five years ago.

Underpinning these achievements are embedded computing systems. Built around specialised chips, these systems are designed to perform specific tasks. Acting like a tiny PC, they can be found in everything from digital cameras and heart pacemakers to robots and aircraft guidance systems.

As the capability and complexity of these embedded systems increases, so does the challenge of ensuring they perform reliably. Just as PCs and servers must be protected from malicious code and external attacks, so too must embedded systems.

The challenge becomes even more complex when these systems are charged with performing multiple tasks or running a range of different software applications, as is already the case in mobile phones. Each must be designed so that, if one function is compromised, the others can continue to run normally.

The NICTA approach

NICTA researchers have focused on three key elements that allow embedded systems to be made more secure and reliable:

- reducing the amount of operating system code (the kernel) that has unrestricted access to the system's hardware
- creating a mathematical model that allows the operating system code to be proven to be reliable; and
- developing a method of measuring and confirming the time taken for the system to perform its required tasks.

Because the operating system kernel has unrestricted access to a device's hardware, reducing the amount of code it contains also reduces the chance of errors and malfunctions. Working with an open source kernel, NICTA researchers have managed to create a microkernel comprising around 10,000 lines of code. This can be used in place of existing embedded operating systems that can be many times that size.

The small size opens up opportunities to achieve an unprecedented degree of reliability assurance – a mathematical proof that the kernel is operating correctly, i.e. is free of bugs. This has the potential to revolutionise the practice of embedded systems development. Work on such a proof is progressing well at NICTA.

Work is underway on compartmentalising the software running on that kernel, so that if one element malfunctions or is compromised, the remainder of the system can continue to operate. This is particularly important in critical embedded systems which must not be allowed to fail. In combination with the correctness proof of the kernel, this will make

it possible to give an embedded system a quality 'stamp', verifying that it can be trusted to work as intended.

Development work is also being undertaken on a second mathematical model that can calculate and confirm the time taken by embedded systems to perform certain tasks. This becomes critical in real-time systems where an inability to complete a task in a given time could have serious repercussions.

For example, a pacemaker unable to process incoming signals could miss a human heartbeat, or a fly-bywire aircraft system could be unable to react quickly enough to pilot commands.

The model calculates the maximum time the system could possibly take to perform a task. Designers and programmers can then ensure that this measure is within operational requirements.

The results

The NICTA Embedded, Real-Time and Operating Systems (ERTOS) program has successfully completed work in each of these areas, and has created the L4/Iguana embedded operating system. L4/Iguana combines the required features of a small amount of microkernel code and the ability to securely encapsulate operating software so that one compromised element cannot adversely affect others.

The team has also achieved world-record performance of its operating system on ARM processors, which are used in many battery-powered embedded systems, such as mobile phones and media players (eg. the iPod). They have developed the capability to run a virtual machine environment for the use of Linux-based software. NICTA researchers are continuing to refine the testing models that will enable the quality and reliability of embedded system code to be mathematically proven. This should be achieved within the next 24 months.

Commercialisation opportunities

NICTA has already signed an agreement with US-based communications electronics company QUALCOMM which plans to use the L4/Iguana operating system in future versions of its communication chipsets for mobile phones. NICTA's leading position in this critical development area positions it well to take advantage of the rapidly growing market for secure embedded systems.

Governments around the world – particularly in Europe – are keen to establish strict requirements for the trustworthiness of embedded systems used in key areas such as defence and national security, or used for processing sensitive personal data. NICTA's testing models, together with the L4/Iguana operating system, places the organisation in a strong position to take advantage of this trend. Research from this project has created the foundation for a NICTA spin-off called Open Kernel Labs.

3