NICTA

Building Effective Operating Systems in Cyber Defence - Now and into the Future

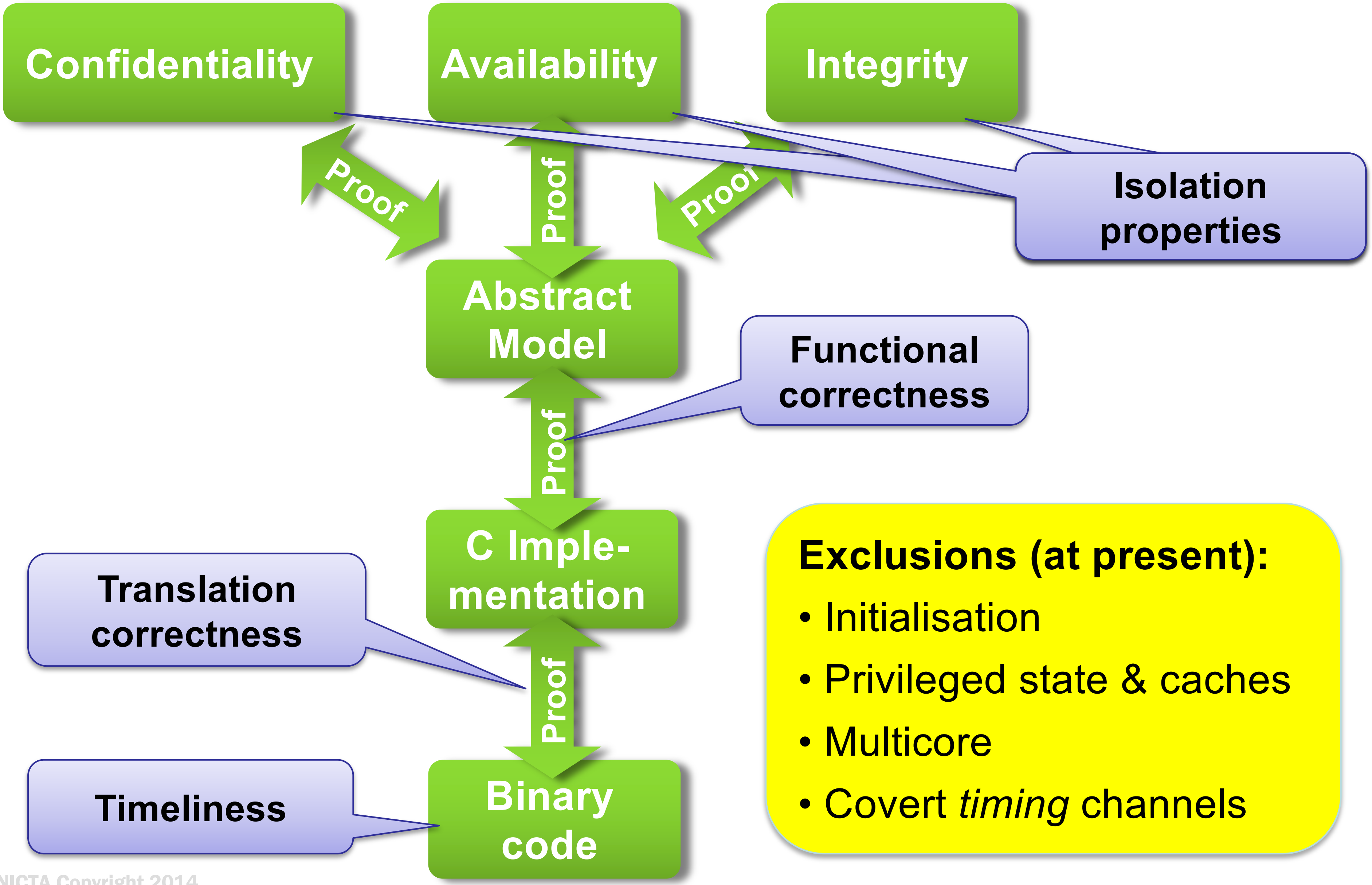
Prof Gernot Heiser

Dr Jodi Steel

Agenda

- What is an ‘effective operating system for cyber defence’?
- Integrating into larger trustworthy systems
  - DARPA HACMS case study
- Implications for ADF and Defence Industry

seL4: Operating System for Cyber Defence



Confidentiality

Availability

Integrity

Proof

Proof

Proof

Isolation properties

Abstract Model

Proof

Functional correctness

C Imple-mentation

Translation correctness

Proof

Binary code

Timeliness

Exclusions (at present):

- Initialisation
- Privileged state & caches
- Multicore
- Covert *timing* channels

Characteristics

What is formal verification?

- Mathematical modelling to reason about properties
- ➢ provable properties with explicit assumptions

seL4

- Protected mode processors (ARM & x86)
- Proof of functional correctness and isolation
- Fastest protected-mode kernel
- Verified interrupt latencies
- Integration of untrusted legacy components

eChronos

- Unprotected microcontrollers
- Proof of functional correctness
- Ultra-low real-time latencies
- Suitable for deeply embedded systems

Evolution to True Trustworthiness

NICTA

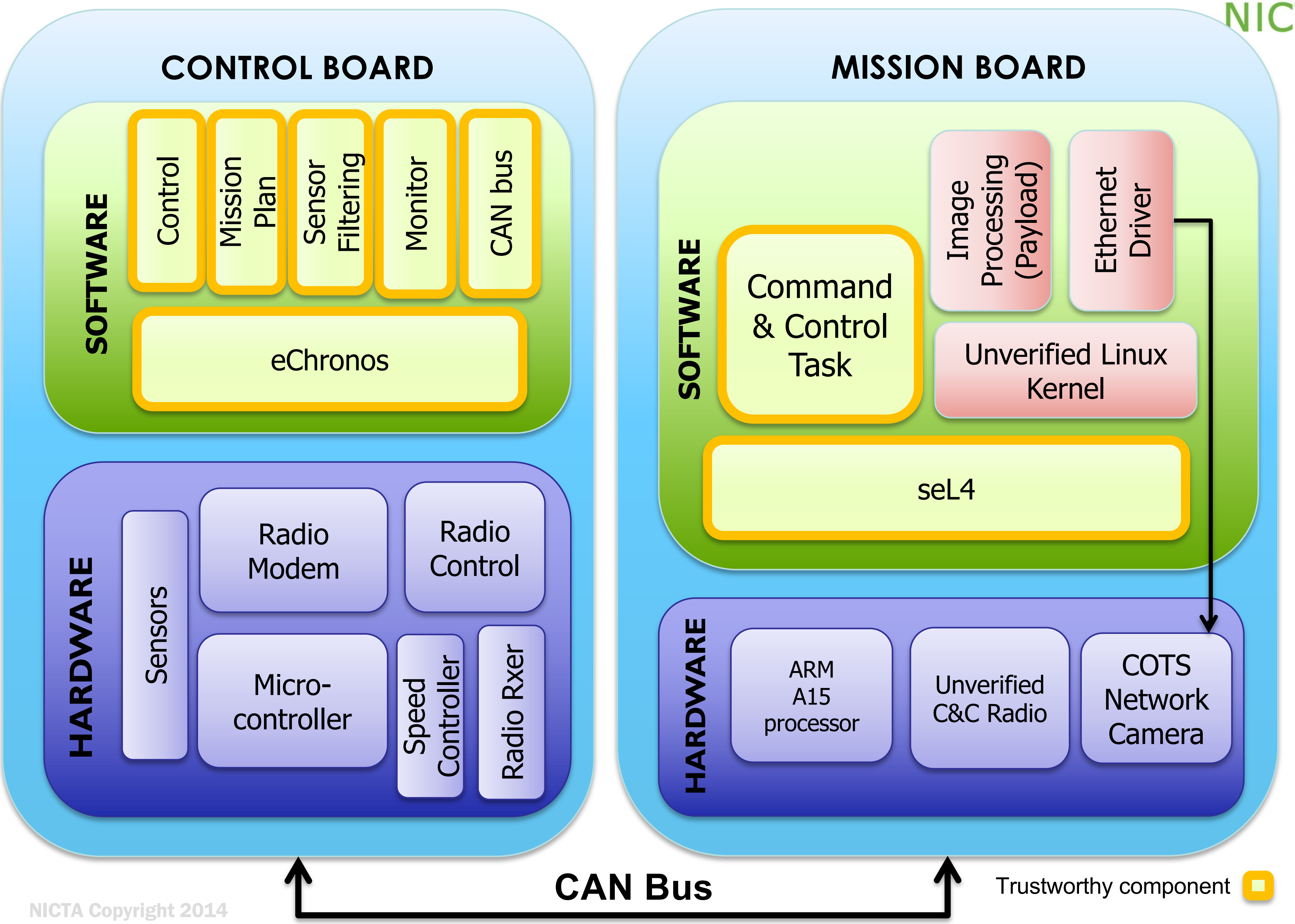
- Operating system necessary but not sufficient
  - Whole system trustworthiness
- Case study: DARPA HACMS
  - Larger trustworthy systems, cheaper and faster
  - Software, tools, demonstrators

BOEING UNMANNED LITTLE BIRD (AH-6)

QUADCOPTER (RESEARCH VEHICLE)

NICTA Rockwell Collins BOEING galois University of Minnesota

Research Vehicle Architecture



Trustworthy component 🟨

Cost of Assurance

Industry Best Practice:

- “High assurance”: $1,000/LOC, no guarantees, *unoptimised*
- Low assurance: $100–200/LOC, 1–5 faults/kLOC, *optimised*

State of the Art – seL4:

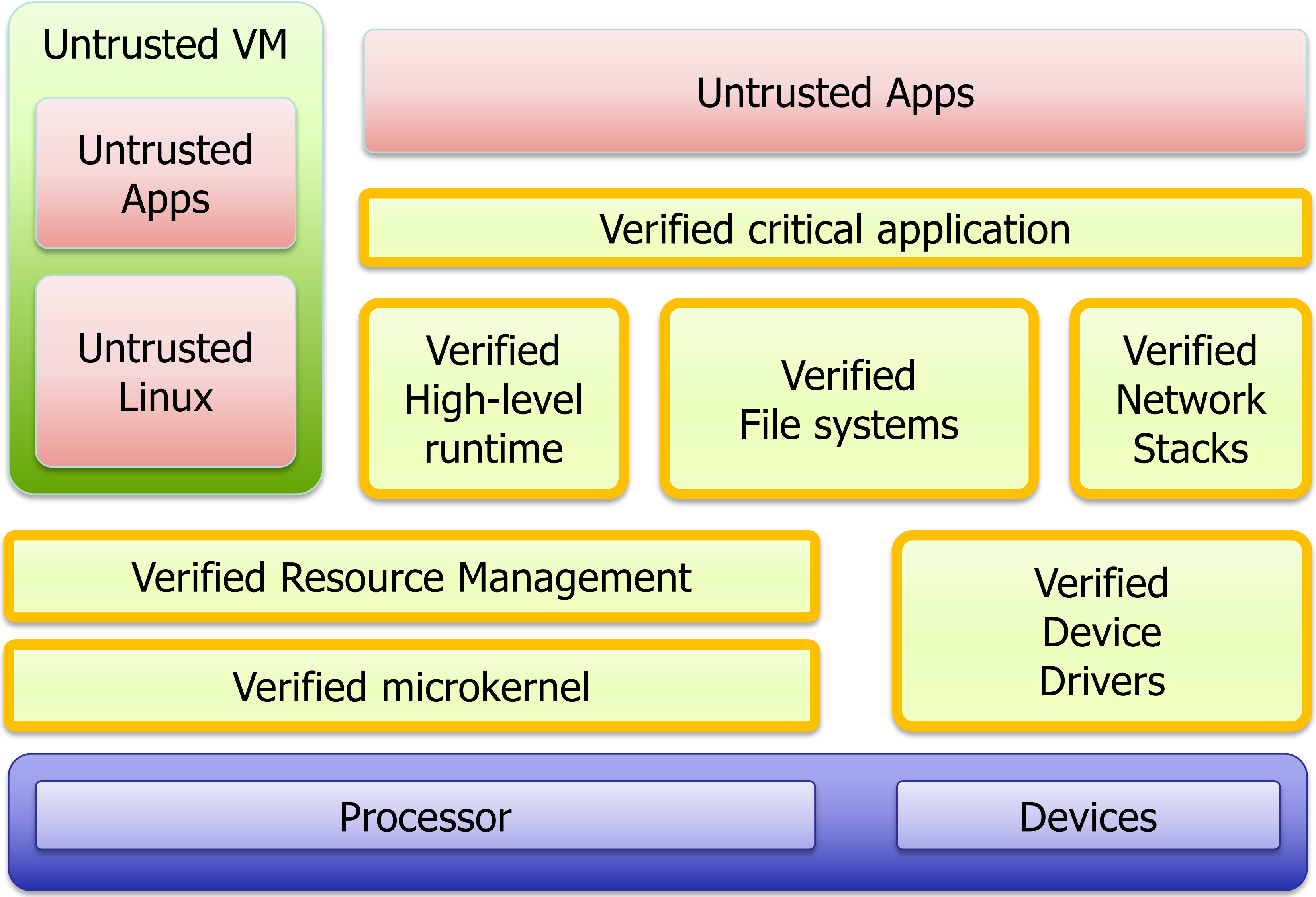
  - $400/LOC, 0 faults/kLOC, *optimised*

- Estimate repeat would cost half
  - that’s about the development cost of the predecessor Pistachio!
- Aggressive optimisation
  - much faster than traditional high-assurance kernels
  - as fast as best-performing low-assurance kernels

Implications for ADF and Defence Industry

- Group is here in Australia
  - critical mass, world leading capability
  - others haven’t caught up
  - Local partners – building more local capability
- seL4 open source release 29 July 2014
  - Dual licensing available
- eChronos available for licencing
- Ready for deployment!

Future: Full-Scale Trustworthy System



Summary

- Evolution to full scale trustworthy systems
  - Cost and time effective
- Critical mass of capability in Australia
- seL4 open source release 29 July 2014
  - Dual licensing available
- eChronos available for licence
- Ready for deployment!

Contacts

Technical:

gernot@nicta.com.au

Business:

Jodi.Steel@nicta.com.au