# Embedded Systems Safety, Reliability and Security: The Challenge of Complexity

Gernot Heiser

NICTA, UNSW and Open Kernel Labs

Australian Government
Department of Communications, Information Technology and the Arts
Australian Research Council

NICTA Members

NICTA Partners

# Embedded Systems are Everywhere

NICTA



Let's think about the implications...

# Lessons from Desktop Systems

NICTA

## Desktop Computers Are Unreliable

- They crash
- They get cracked
- They get infected



How about embedded systems?

# Modern Embedded Systems (ES)

NICTA

- Ubiquitous
  - dozens per person, part of everyday life
- Increasingly dependent on correct operation
  - security of data
    - protection of personal information
    - protection of valuable media content
  - device safety
    - faulty devices can injure or kill
    - faulty devices can interfere with wireless networks
  - device reliability
    - user: annoyance, opportunity cost to business
    - manufacturer: cost to reputation, cost of recalls

# Technical Challenges of ES

NICTA

- Embedded-systems functionality is exploding
- Software complexity is growing strongly
  - millions of lines of code
  - gigabytes of embedded software
- Complexity is the enemy of reliability
  - trustworthiness becomes harder to achieve
- Many embedded systems become open
  - user-installed untrusted software
- Faults require remote software upgrades
  - increased security problems
- Software cost requires component reuse across domains
  - especially OS software, comms stacks, GUIs, etc

# Research Policy Challenges

- ES reliability essential for functioning of the future society
- There must be a *research focus on ES reliability*
- The technical issues relate to the areas of:
  1. computer architecture
  2. operating systems
  3. software engineering
  4. formal methods
  5. systems engineering
- A successful research policy must *integrate* all 5 disciplines
  - This is a considerable challenge!

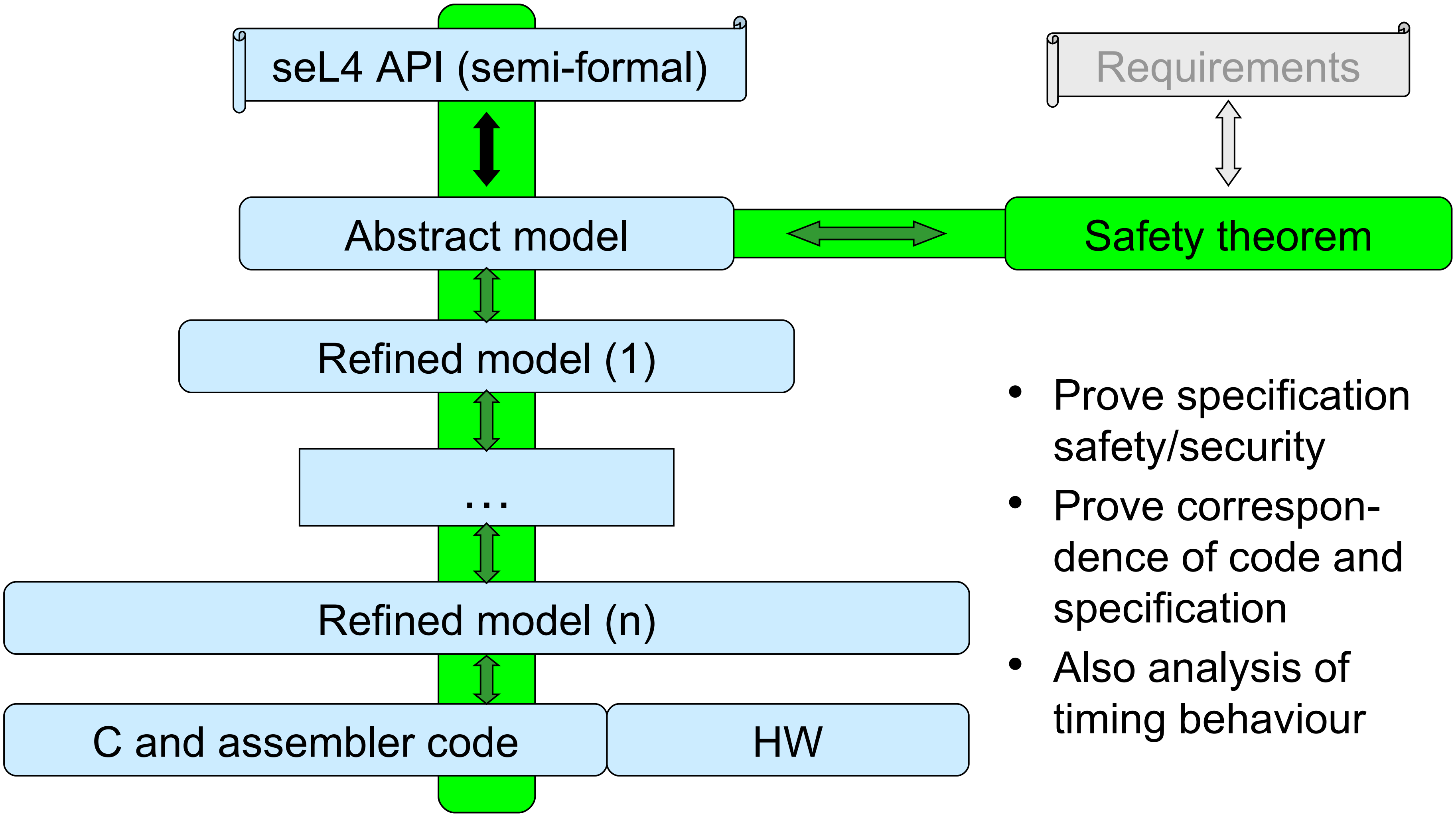
# NICTA

- National Centre of Excellence for ICT Research
- Publicly-funded not-for-profit organisation
- Taking leadership in defining national ES research agenda
- World-class research in-house and in affiliated universities
- Well networked with industry
  - local industry
  - European ARTEMIS framework
  - strong commercialisation pipeline for own research

# NICTA's ES Research Strategy

- Overall strategy: Reliability through:
  - small, ultra-reliable foundation
  - design by composition
  - formal reasoning
- Step 1: Combine operating systems and formal methods
  - small, high-performance microkernel
  - formal verification to ensure correctness

# Formally-Verified OS Microkernel



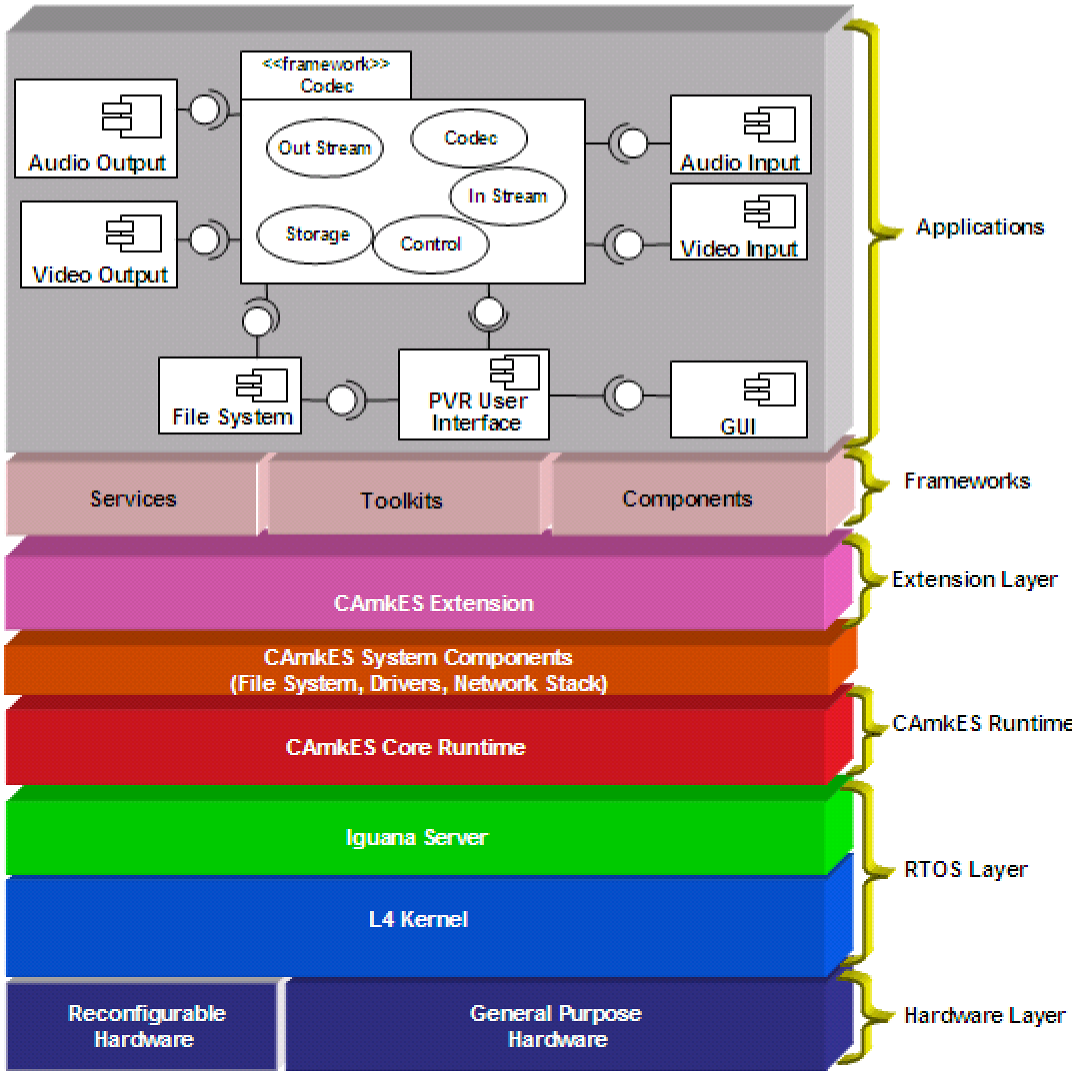

- Prove specification safety/security
- Prove correspon-dence of code and specification
- Also analysis of timing behaviour

# NICTA's ES Research Strategy

- Overall strategy: Reliability through:
  - small, ultra-reliable foundation
  - design by composition
  - formal reasoning
- Step 1: Operating systems (OS) and formal methods (FM)
  - small, high-performance OS microkernel
  - formal verification to ensure correctness
  - mostly completed, ready for commercialisation
- Step 2: OS and FM and Software Engineering (SE)
  - component technology based on verified microkernel

# Component Framework

- Supports highly-componentised software
- Strong protection
  - kernel guarantees interfaces
- Low overheads
- Suitable for formal reasoning about components



# NICTA's ES Research Strategy

- Overall strategy: Reliability through:
  - small, ultra-reliable foundation
  - design by composition
  - formal reasoning
- Step 1: Operating systems (OS) and formal methods (FM)
  - small, high-performance OS microkernel
  - formal verification to ensure correctness
  - mostly completed, ready for commercialisation
- Step 2: OS and FM and Software Engineering (SE)
  - component technology based on verified microkernel
  - formal reasoning about interaction
  - non-formal requirements (time, power)
  - part done (w/o FM), strategy being defined

# NICTA's ES Research Strategy

- Overall strategy: Reliability through:
  - small, ultra-reliable foundation
  - design by composition
  - formal reasoning
- Step 1: Operating systems (OS) and formal methods (FM)
- Step 2: OS and FM and Software Engineering (SE)
- Step 3: OS + FM+ SE+ Systems Engineering
  - no strategy yet
  - significant local expertise
  - but international collaboration required
    - involving private and public sector

# NICTA's ES Research Strategy

NICTA

- Missing part: Computer architecture
- Reason: cannot influence from Australia
- Who can?
  - dominant player: US
    - but focussed on high-end and unsuitable architectures
  - also in the game: Europe (ARM, ST) and Japan
    - significant focus on ES
  - emerging players: China and India
    - potential for major impact
- We are willing to cooperate!

# Summary

- Embedded systems reliability is a huge technical challenge
- Addressing it requires research policy that
  - combines and integrates disciplines
  - combines private and public sector
  - encourages and supports international cooperation
- We believe that NICTA has taken steps in the right direction
- More needs to be done