IoT Security – A Hopeless Case ?

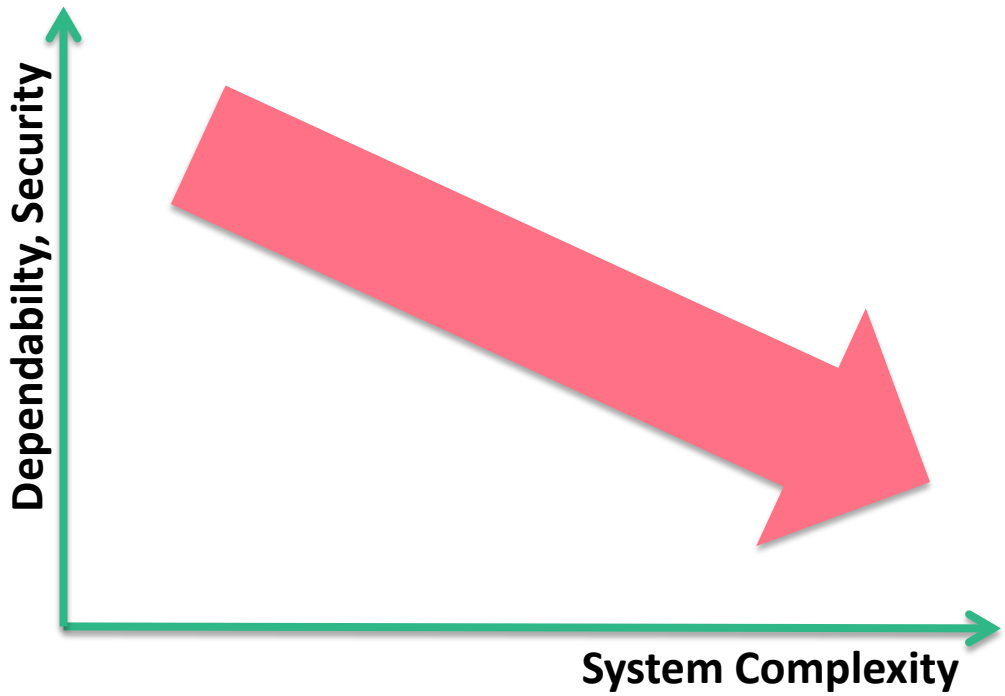
Gernot Heiser | gernot.heiser@data61.csiro.au | @GernotHeiser
Trustworthy Systems | Data61

April 2017

www.data61.csiro.au

Connected Device Security – An Oxymoron?

Failure Reason 1: Complexity



Complexity Drivers

- Features/functionality
- Legacy reuse

Example Linux

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CU

RISK ASSESSMENT —

Unsafe at any clock speed: Linux kernel security needs a rethink

Ars reports from the Linux Security Summit—and finds much work that needs to be done.

J.M. PORUP (UK) - 9/27/2016, 10:57 PM

The Linux kernel today faces an unprecedented safety crisis. Much like when

Failure Reason 2: Care Factor

Developer priorities

1. Features/functionality
2. Cost
3. Time to market
4. …
5. …
6. …
7. …

…. …

…. …

999.Security

Developer expertise

1. Undergraduate programming
2. Application domain
3. Maybe hardware
4. …
5. …
6. …
7. …

…. …

999.Security

So, Let's All Use Java

… or other type-safe languages

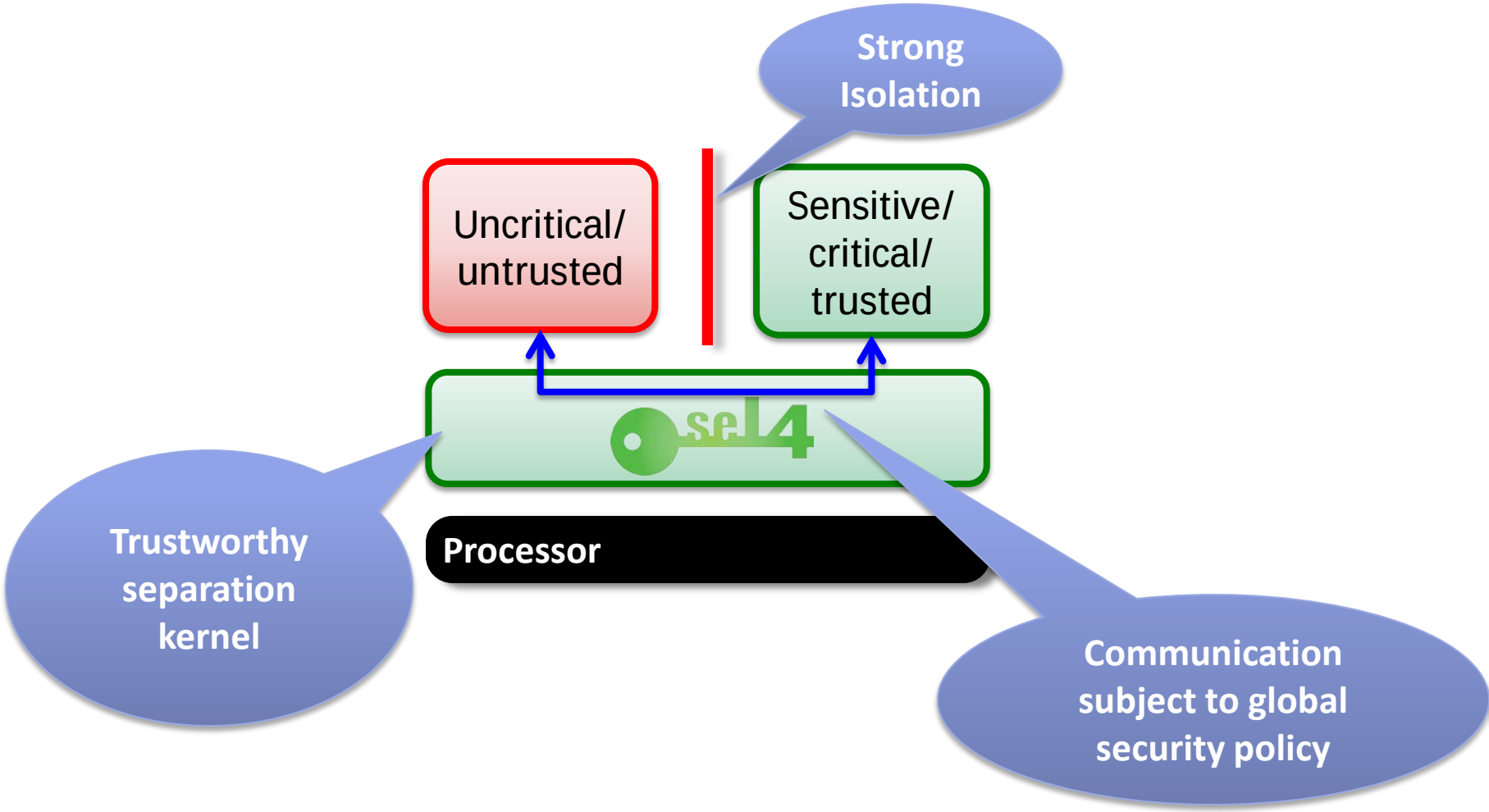
- Type-safe languages eliminate many security-critical faults
  - Buffer overflows
  - Conversion errors
  - Aliasing problems

- But:
  - Overhead is often not bearable, e.g. reduces battery life
  - Interfacing to hardware often requires "unsafe" coding
  - Doesn't help with legacy code

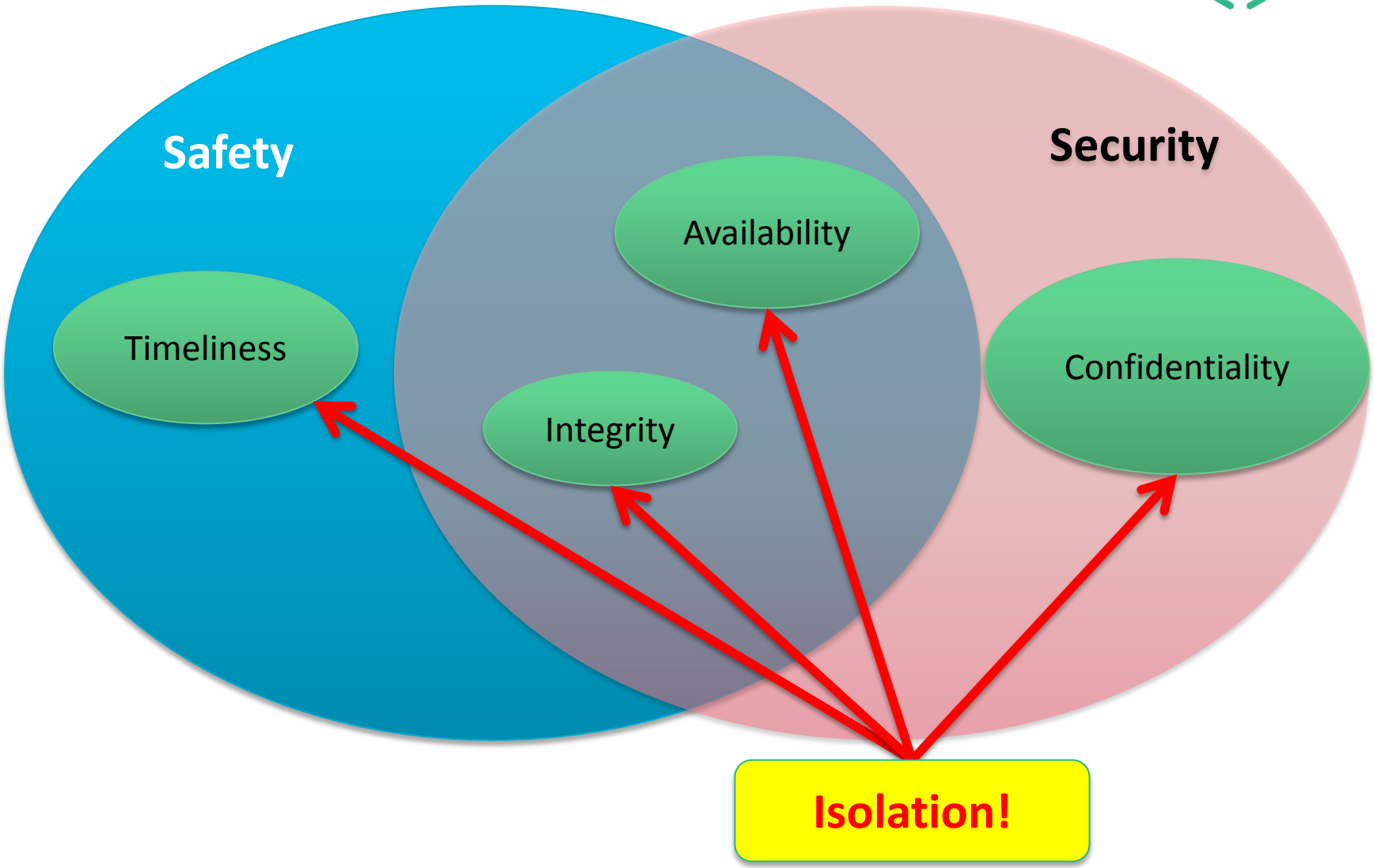
OK, Let's Use a Fire Wall

- Imposes overhead (reduces battery life)
- Even more code – may *increase* attack surface
- No help for valid messages that trigger bugs in software

Fundamental Security Requirement: Isolation



Isolation for Trustworthiness



Can We Rely on Isolation?

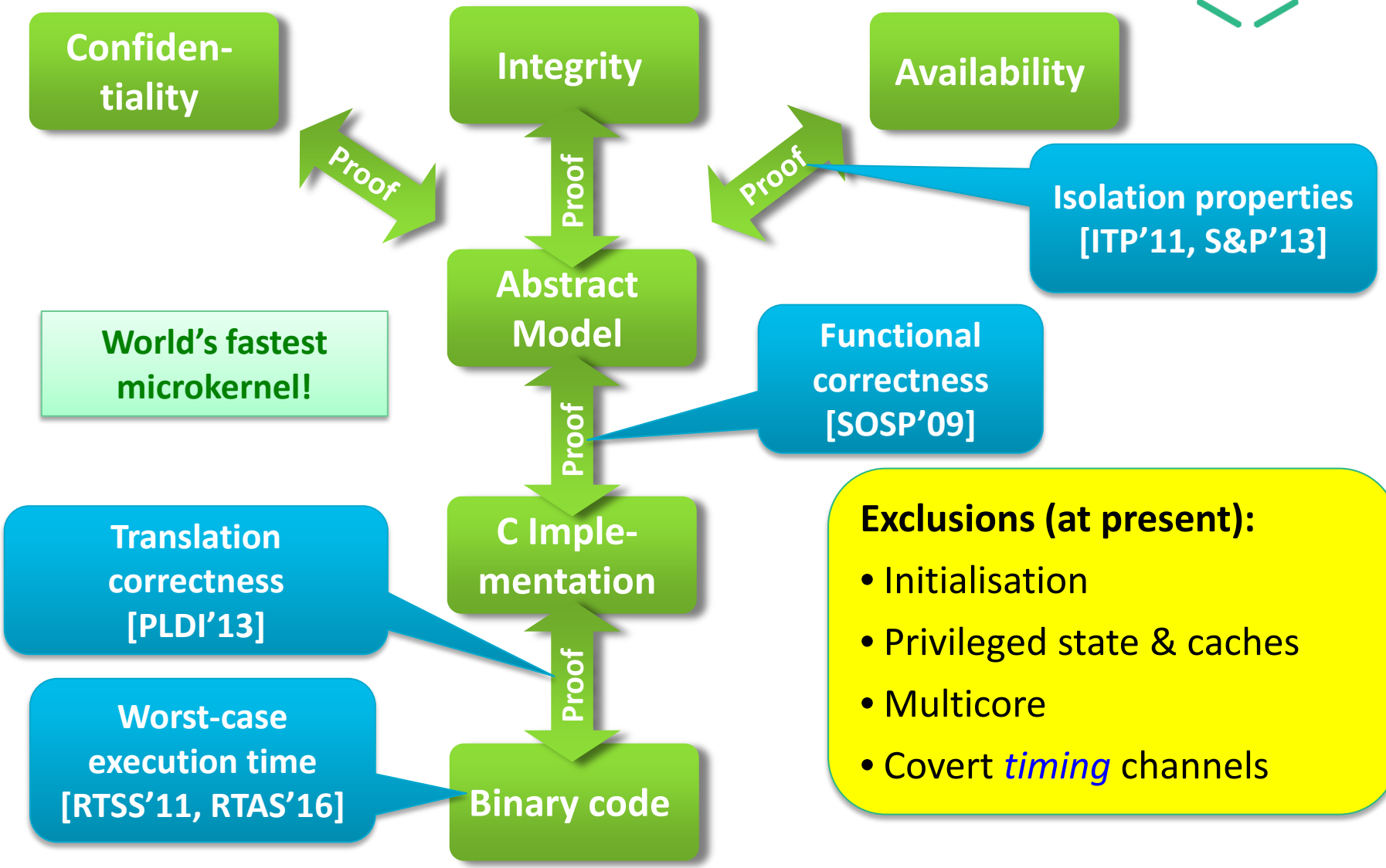
***Claim*:**

A system must be considered *untrustworthy* unless *proved* otherwise!

Corollary [with apologies to Dijkstra]:

Testing, code inspection, etc. can only show *lack of trustworthiness*!

seL4 OS Microkernel: Provable Isolation



Exclusions (at present):

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

Critical Systems: DARPA HACMS

Boeing Unmanned Little Bird

Retrofit existing system!

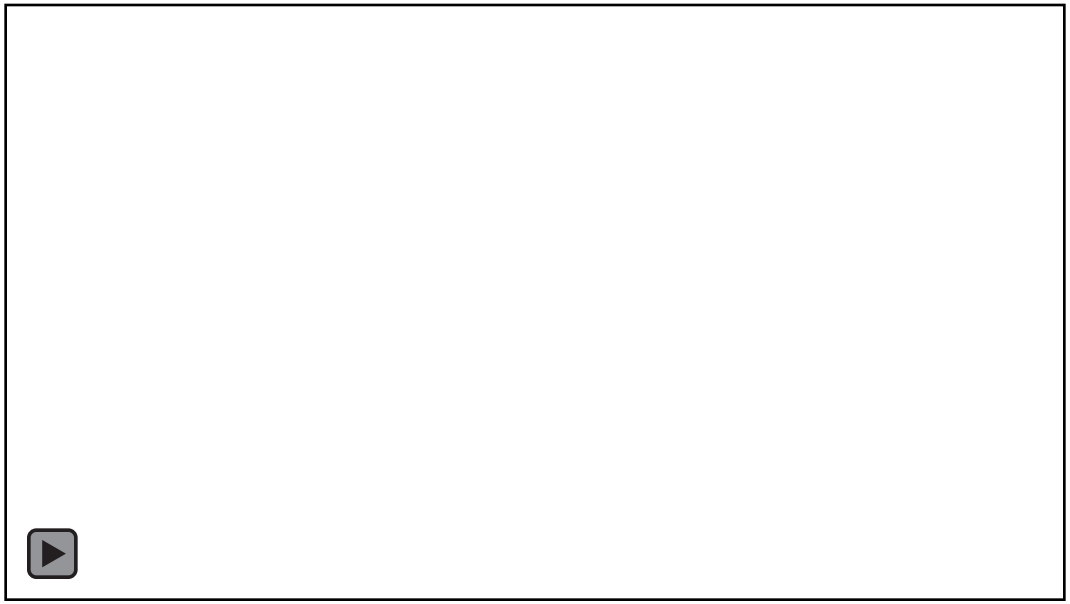
US Army Autonomous Trucks

SMACCMcopter Research Vehicle

Develop technology

TARDEC GVR-Bot

Mesa, AZ, 24 July 2015



sel4 Inside!

DATA 61

Thank you

Security is no excuse for poor performance!

Gernot Heiser | gernot.heiser@data61.csiro.au | @GernotHeiser
APril 2017

http://sel4.systems

sel4

CSIRO