The SICS Hypervisor project for ARM project

Arash Vahidi
SICS Security Lab (SEC)

SWEDISH ICT SICS

What is this all about?

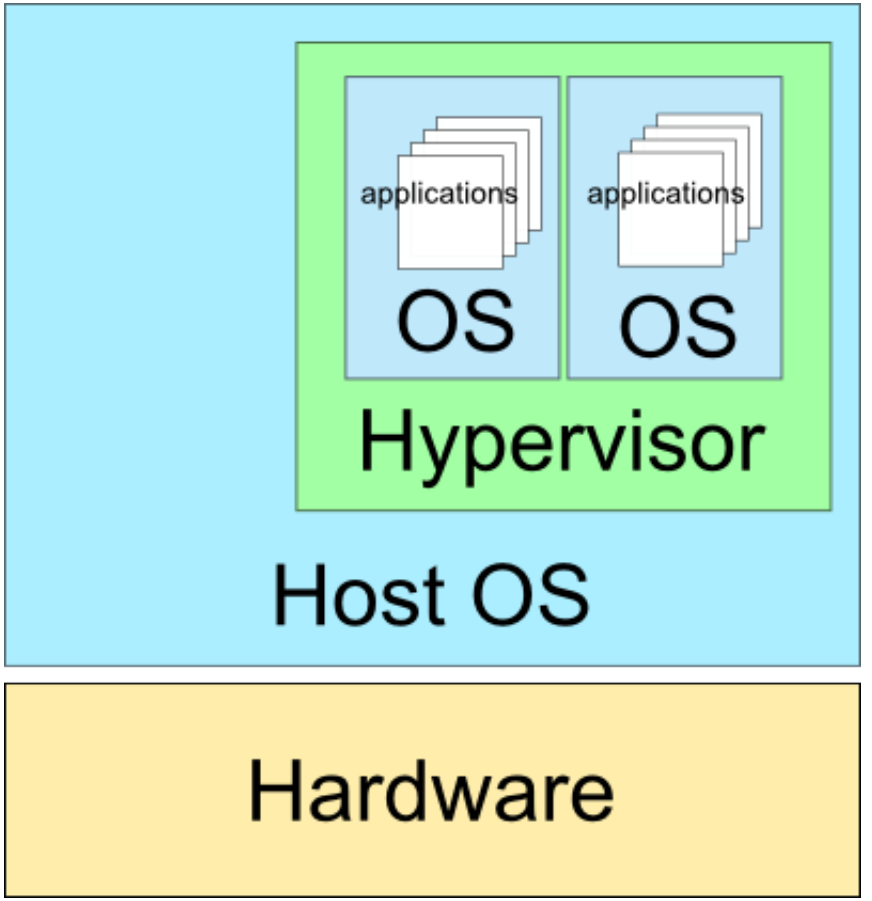
- Embedded systems are getting more and more **complex**,
- **Security** issues are becoming critical,
- Virtualization technologies may be used as a security **enabler**.

What is a hypervisor?

And a few words about the SICS hypervisor...

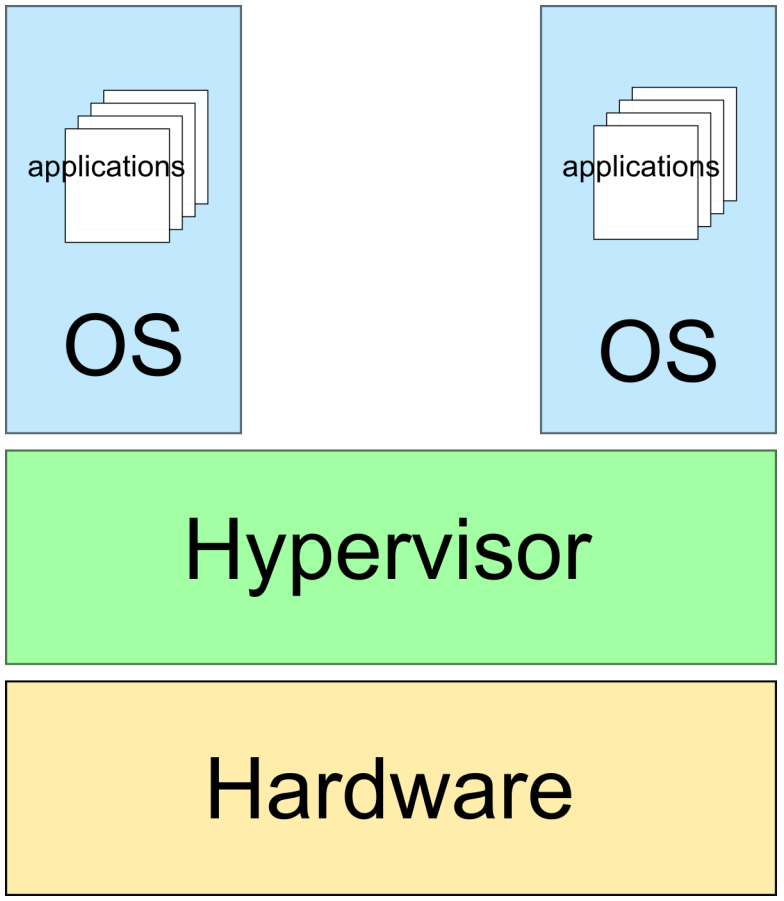
Virtualization?

Virtualization?

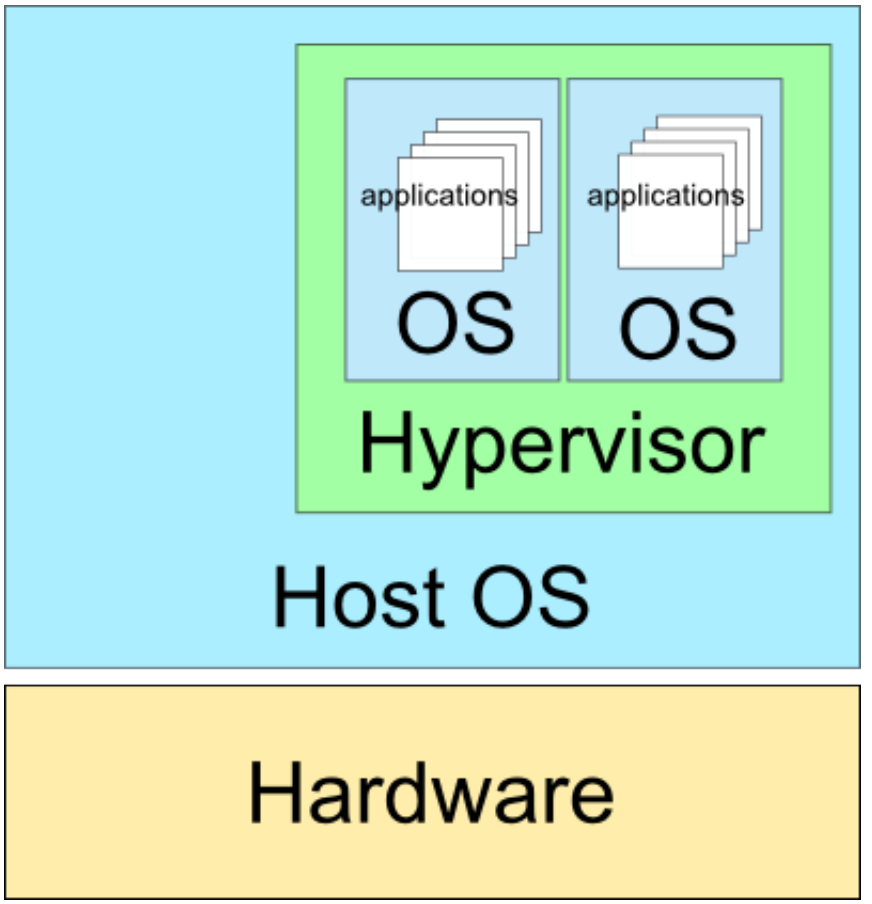


Type 2

Virtualization?

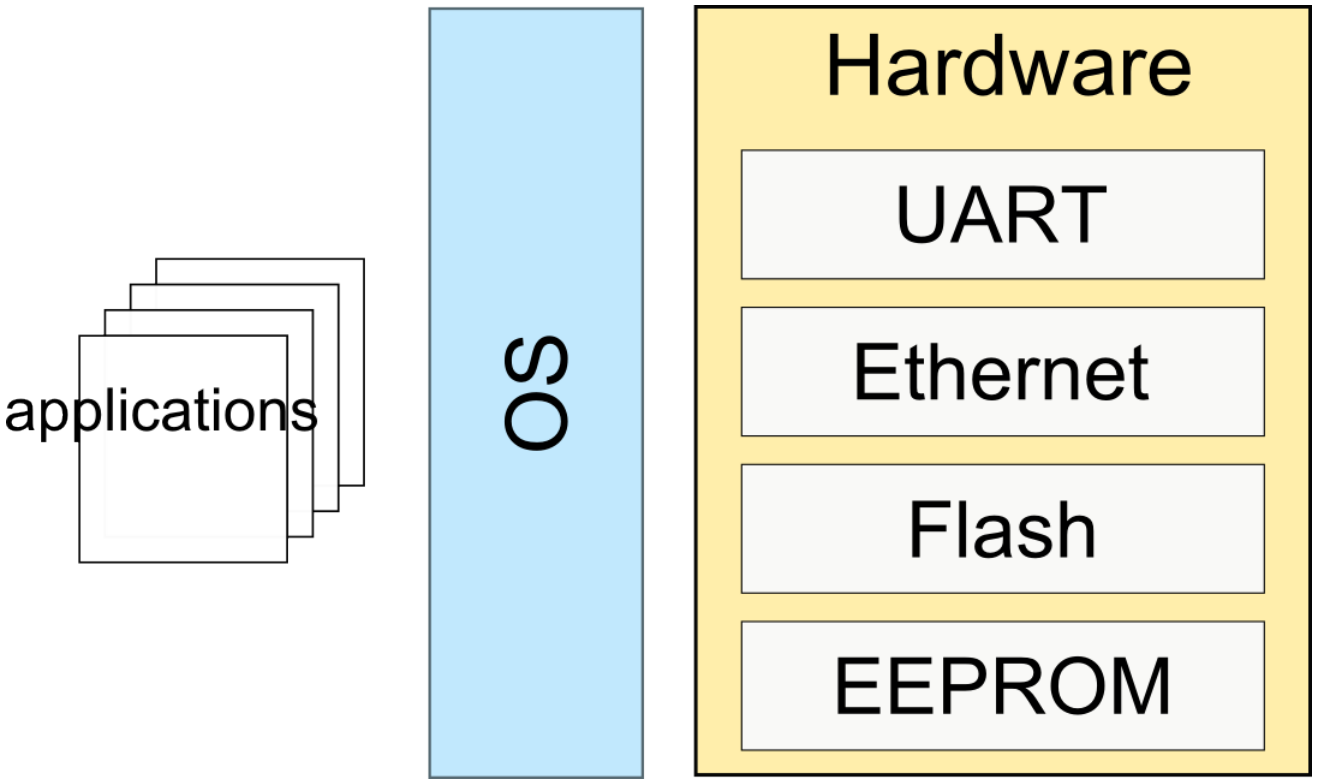


Type 1

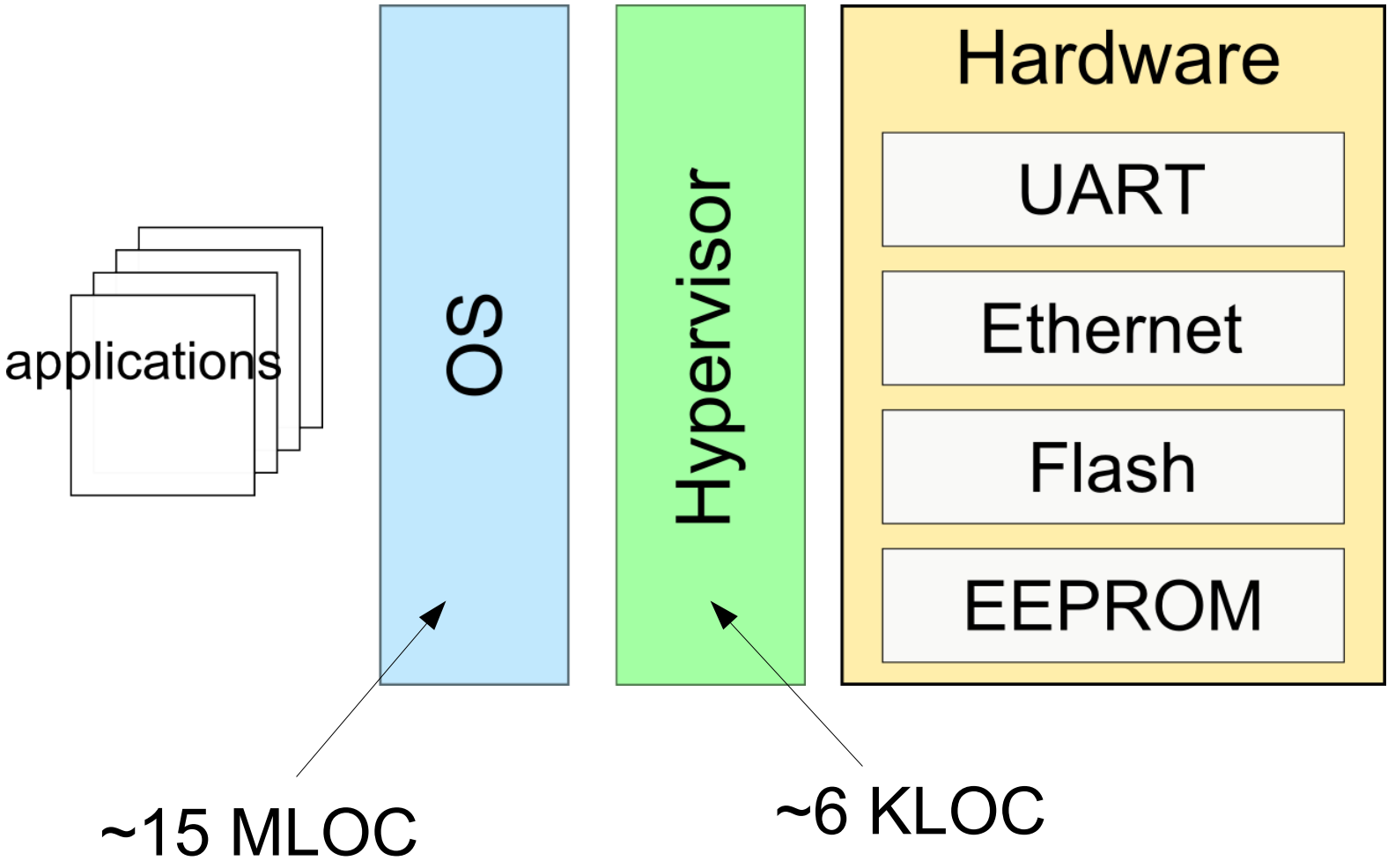


Type 2

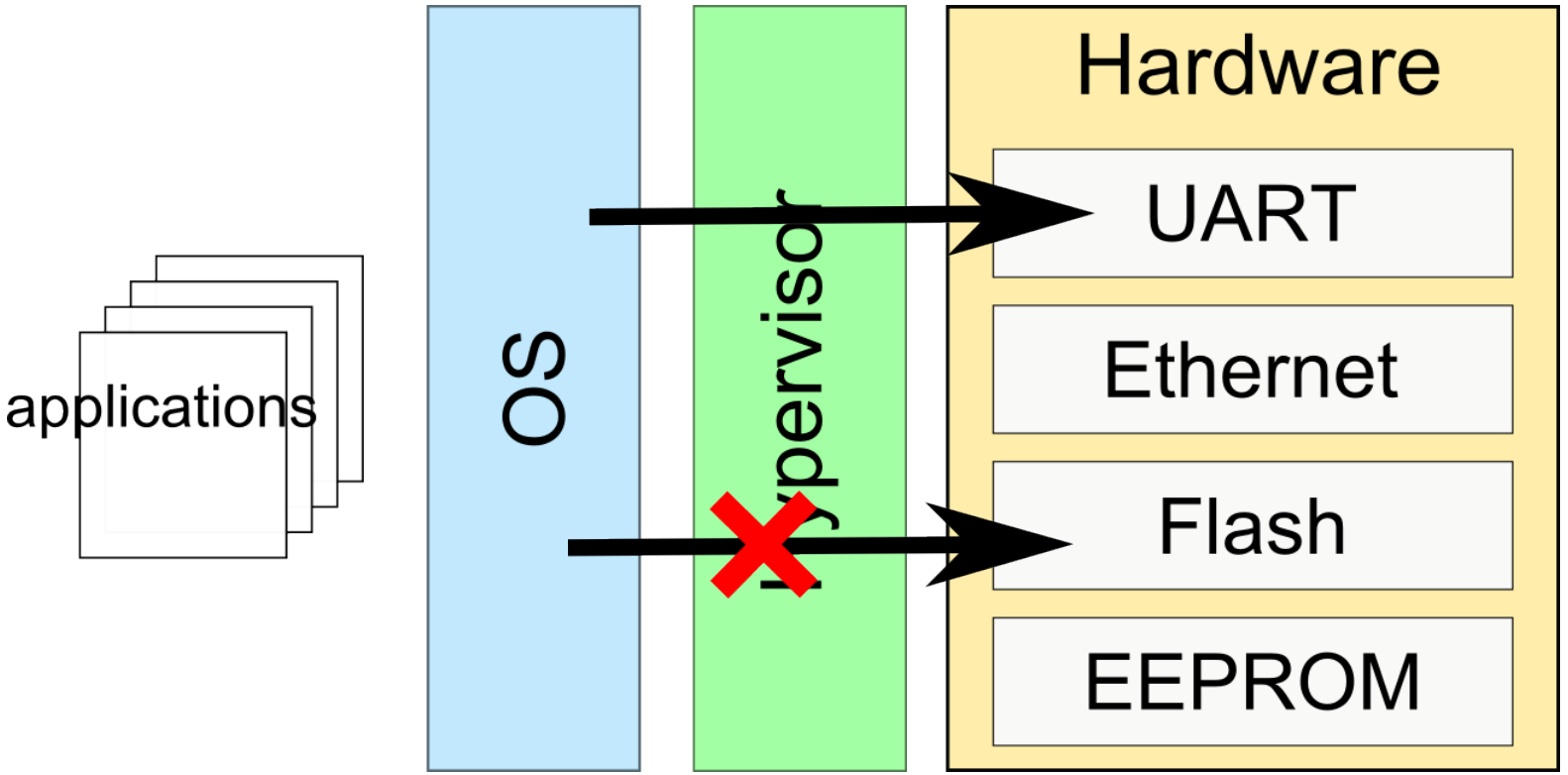
Uses of hypervisors (1)



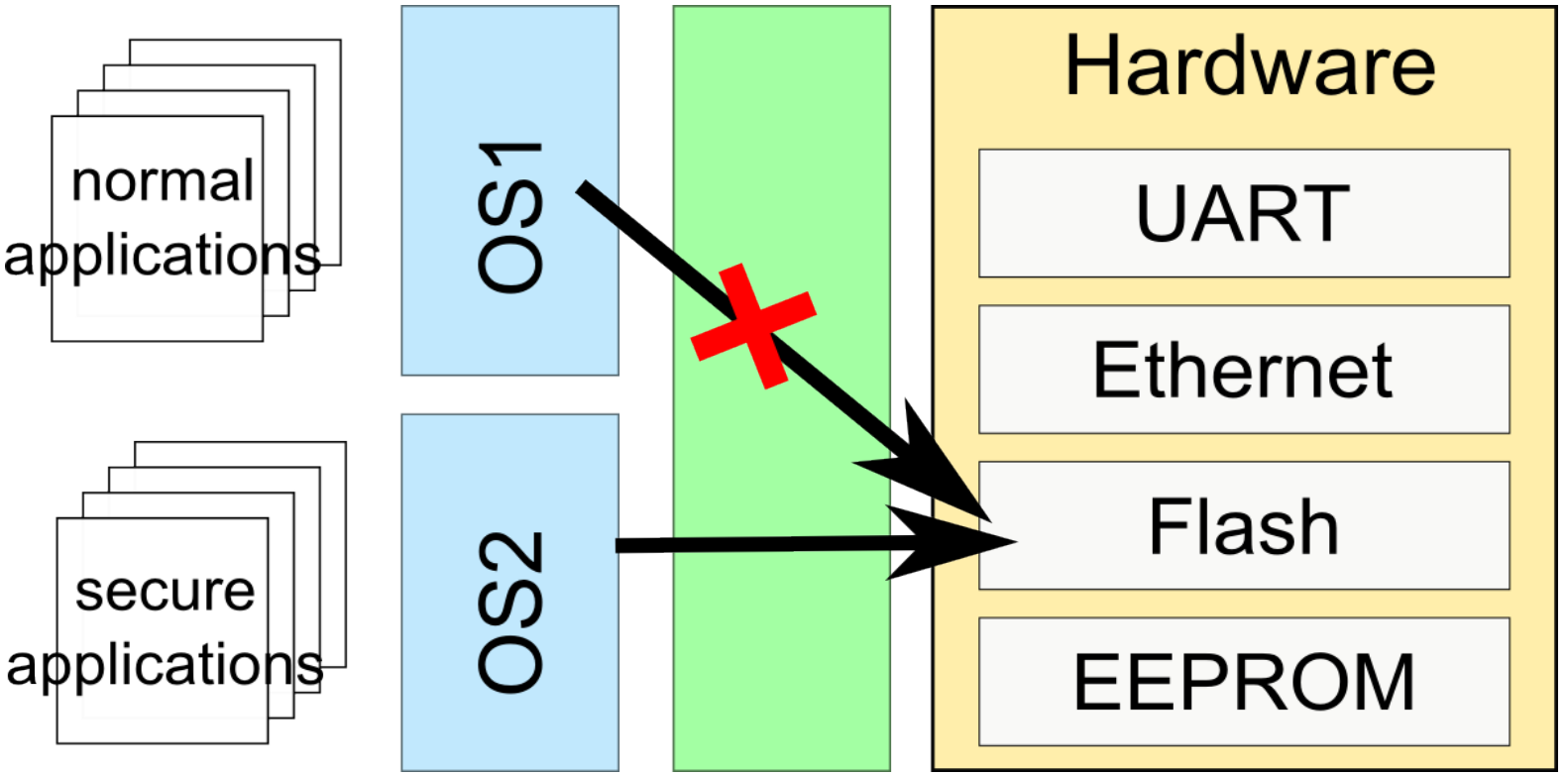
Uses of hypervisors (2)



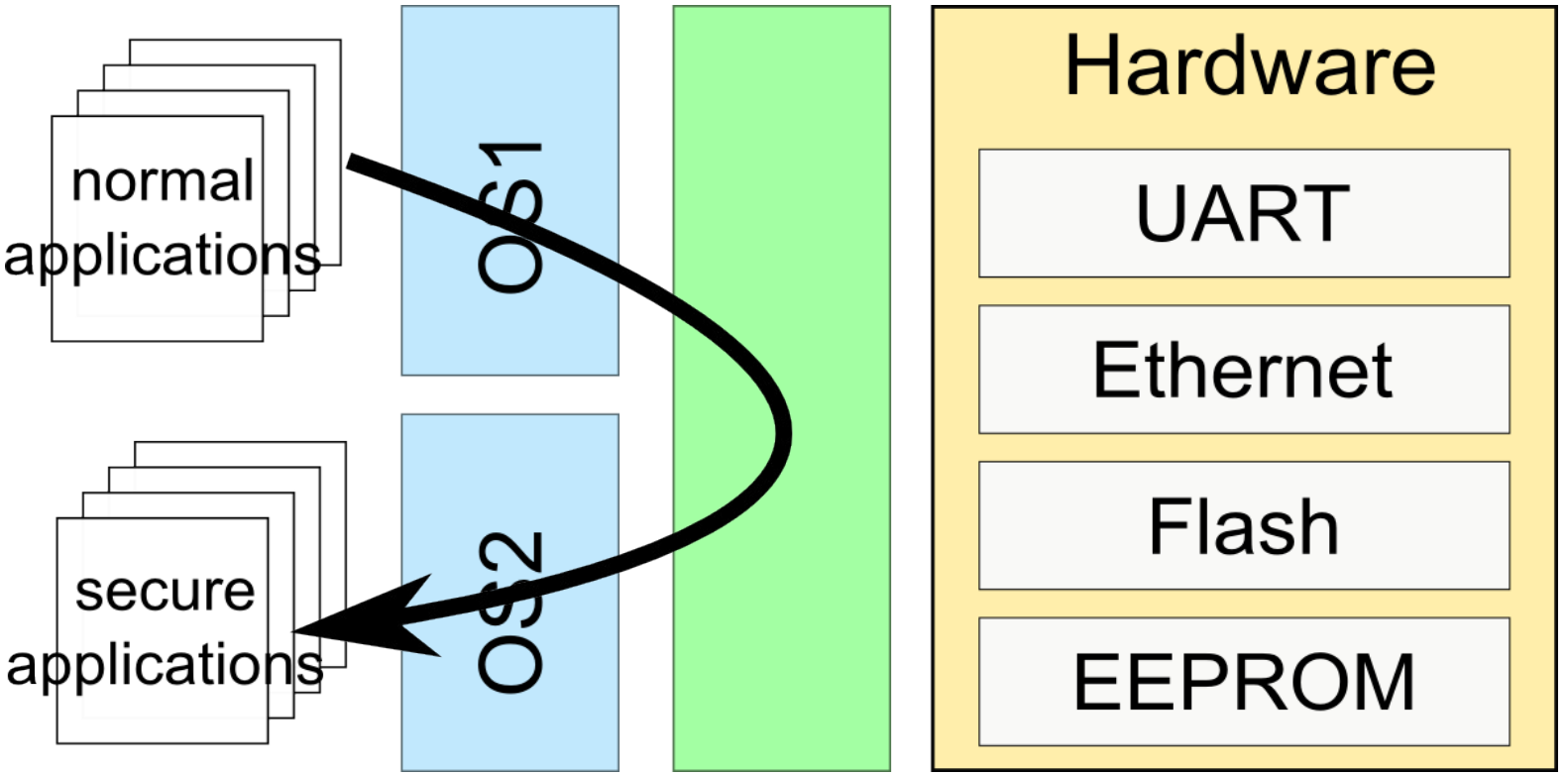
Uses of hypervisors (3)



Uses of hypervisors (4)



Uses of hypervisors (5)



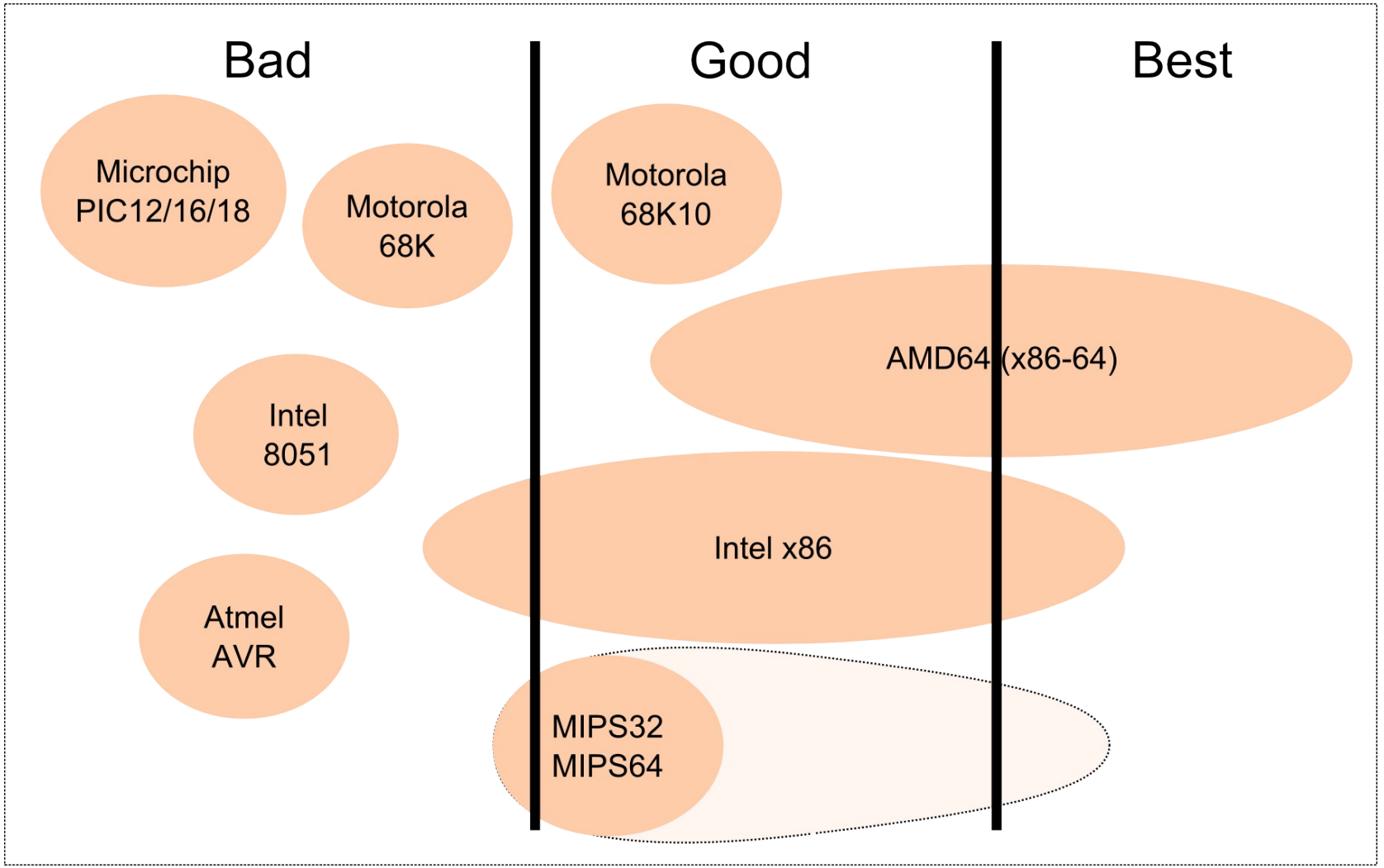
GLOBALPLATFORM™

Hypervisor requirements.

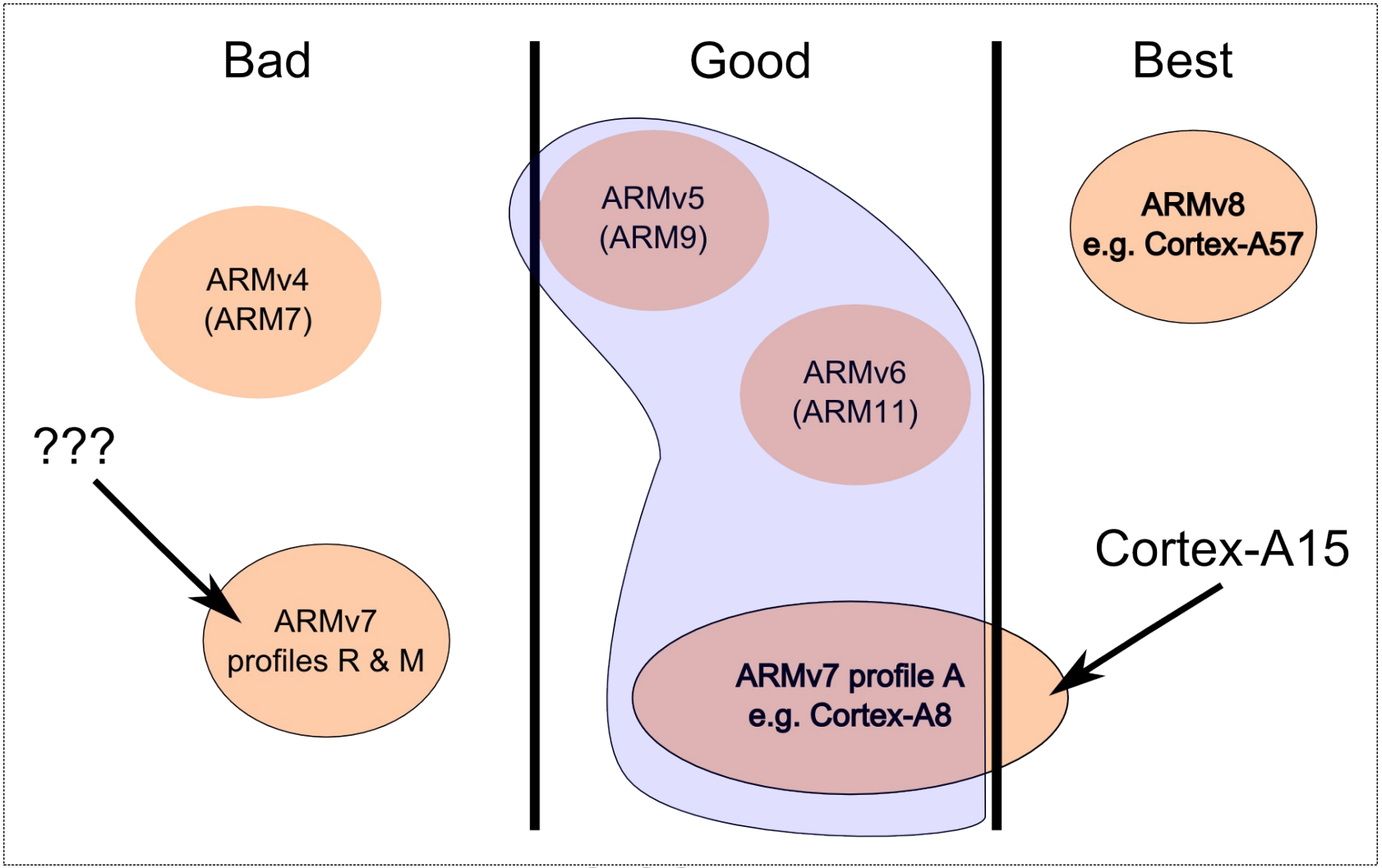
or

Can I use this in my current project?

Virtualization requirements (1)



Virtualization requirements (2)



SICS hypervisor
primary targets

SWEDISH ICT SICS

So there is no free lunch...

What are the costs of virtualization?

Performance degradation?

- Virtualization introduces an overhead
- Virtualization does affect your real-time performance slightly (added latency)
- Depending on the system and the application, this overhead can be significant or negligible
- *SICS hyprevisor: a 2-20% increase of running time was measured in various applications*

Hypervisor footprint?

- Unless for very small systems, the added footprint of a hypervisor is negligible.
- *SICS hyprevisor: a 8-32KB code, 4KB - 1MB memory on ARM.*
- ARM Virtualization Extensions can significantly reduce these numbers (i.e. Cortex-A15 and newer).

Code complexity?

- The hypervisor itself is tiny (few KLOC, we have seen as little as 600 LOC in research versions).
- The guest OS can be run on top of the hypervisor without any modification. This could however result in very poor performance.
- With some changes to the guest OS, one may increase the performance significantly.
  - *For a 2.6 Linux kernel, these modification can be as little as **800** LOC*. Newer kernel versions may require even less changes!

How about MIPS, PPC, XYZ?

- Hypervisors are inherently platform dependent
- However, we have done our best to make the SICS hypervisor easy to port
  - ARM
  - MIPS in progress
- Talk to me if you are working with other architectures

THE END

Questions?