



# The Benefits of Virtualization

*Tony Webb*

*Advanced Automotive Electronics  
Conference 2011*

# Agenda

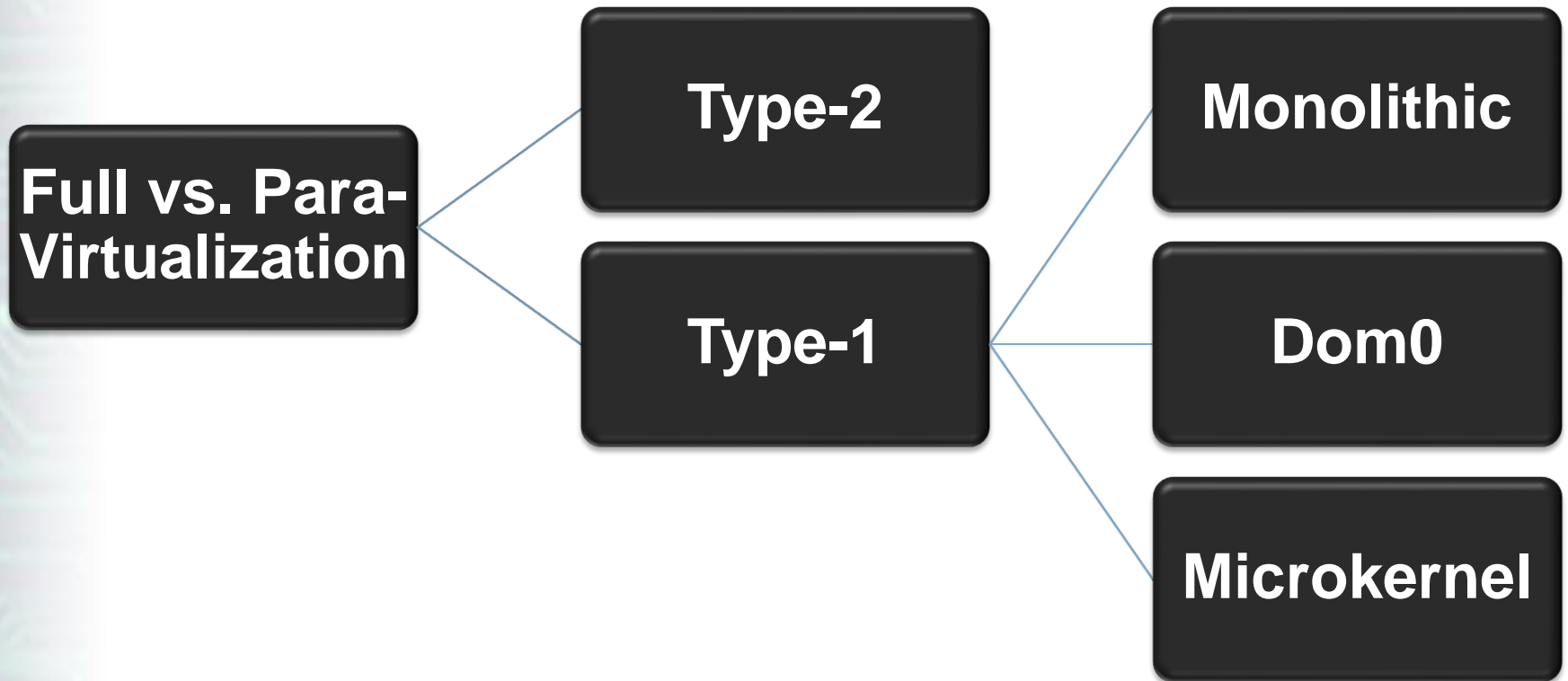
---

- ❑ System Virtualization Techniques for Embedded
- ❑ Types of Hypervisors
- ❑ Latest Embedded Processor Support
- ❑ I/O Virtualization Challenges
- ❑ Embedded Use Cases

# How Does It Work

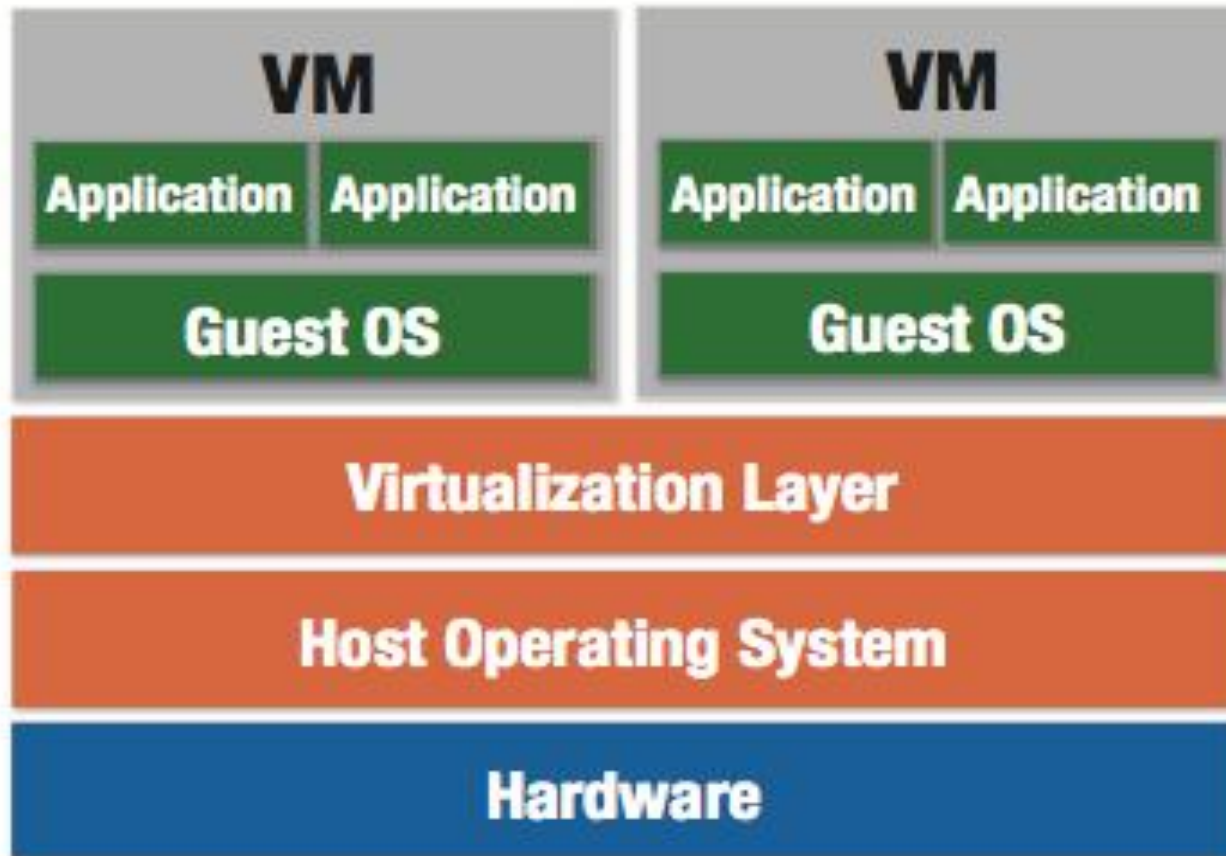
- ❑ By inserting a hypervisor between the HW & guest OS.
- ❑ The hypervisor presents each guest OS with a VM.
- ❑ A VM functions as if it were a dedicated HW platform.
- ❑ The VMs allow the hypervisor to monitor and manage the execution of each guest OS.
  - Manage access to I/O devices.
  - Dictates which areas of memory and storage are available.

# System Virtualization Taxonomy



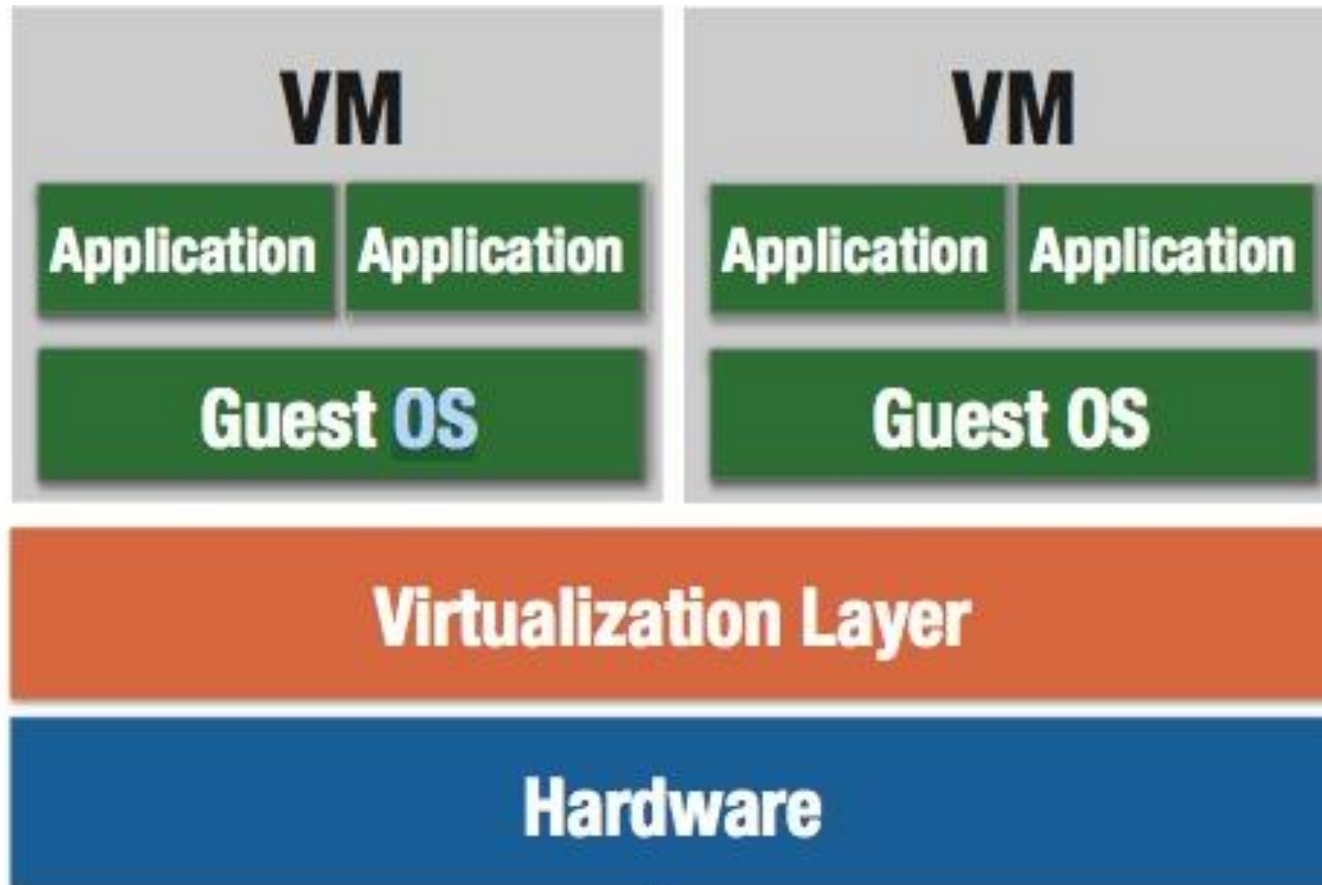
# Type-2 Hypervisor

A Type-2 hypervisor runs on top of a host OS.



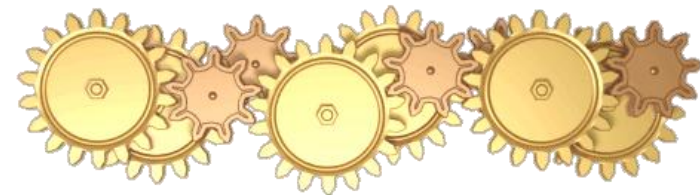
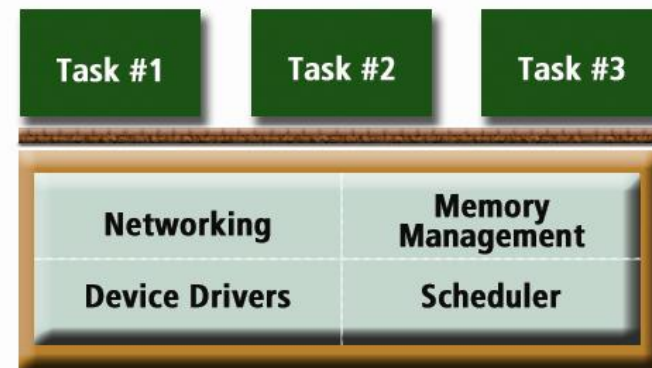
# Type-1 Hypervisor

A Type-1 hypervisor replaces an OS



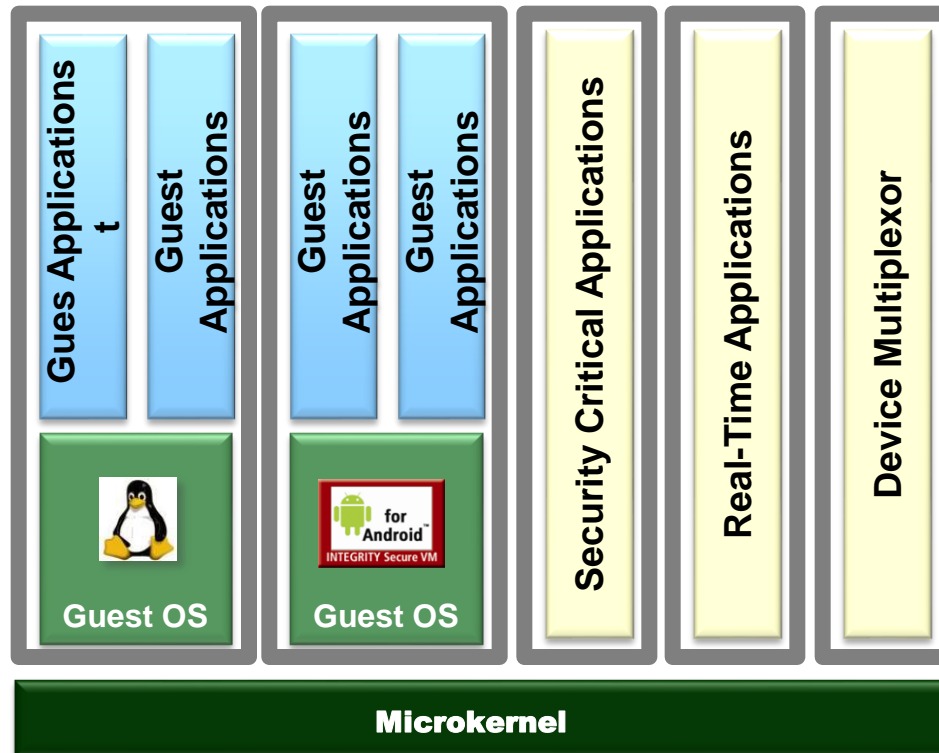
# What am I?

- ❑ Partition and protect memory resources
- ❑ Secure access control for I/O and other system objects
- ❑ Interprocess communication (IPC)
- ❑ Schedule workloads securely and efficiently across cores
- ❑ Power management
- ❑ Device drivers
- ❑ Handle disparate workloads – real-time and general purpose
- ❑ Health monitoring / high availability
- ❑ ***This is what a microkernel already does extremely well***



# Microkernel Type-1

- ❑ Very small TCB
- ❑ Examples: Green Hills Multivisor, Lynuxworks LynxSecure, Sysgo PikeOS



# Hardware Support – Intel

## □ VT-x

- All “dangerous” instructions trapped by hardware
- Selective non-faulting access to privileged state
  - Interrupts/system calls, privileged registers directly handled by guest supervisor
- 2x performance improvement vs. pre-VT
- Page table handling slow
  - Addressed with VT-x2 - EPT
- No I/O DMA protection

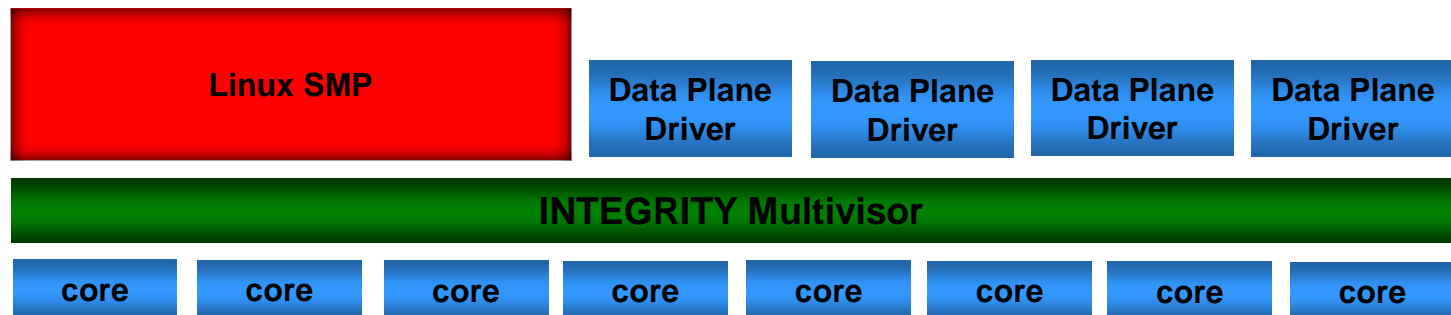
## □ VT-d

- I/O DMA protection
  - I/O devices can be “assigned” to VM
  - I/O device can’t access memory outside domain
- But allowing unfettered guest control of device is dangerous

## □ Atom has VT-x but not VT-d nor VT-x2

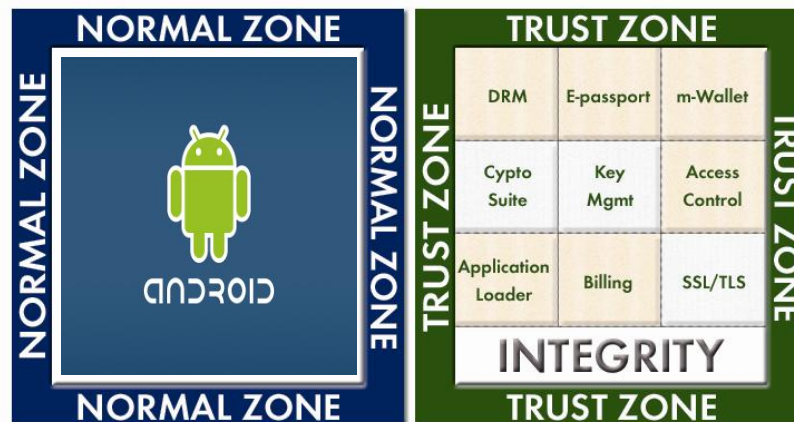
# Hardware Support – Freescale P3/P4/P5

- ❑ Implements Power ISA 2.06 Hypervisor features
  - Hypervisor mode / guest state
  - Interrupt redirection
  - Software-managed TLB
  - [http://www.power.org/resources/downloads/PowerISA\\_V2.06\\_PUBLIC.pdf](http://www.power.org/resources/downloads/PowerISA_V2.06_PUBLIC.pdf)
  - [http://www.power.org/resources/downloads/Power.org\\_White\\_Paper\\_Hypervisors.pdf](http://www.power.org/resources/downloads/Power.org_White_Paper_Hypervisors.pdf)
- ❑ Adds IOMMU (called the “PAMU”)
- ❑ 4-8 cores



# Hardware Support: ARM TrustZone®

- ❑ Trustworthy hypervisor/OS managing “secure zone”
  - Reduce device compliance certification time and cost
- ❑ MMU partitioning further reduces certification burden
- ❑ Alternative to traditional hardware hypervisor mode
  - Very fast for single guest



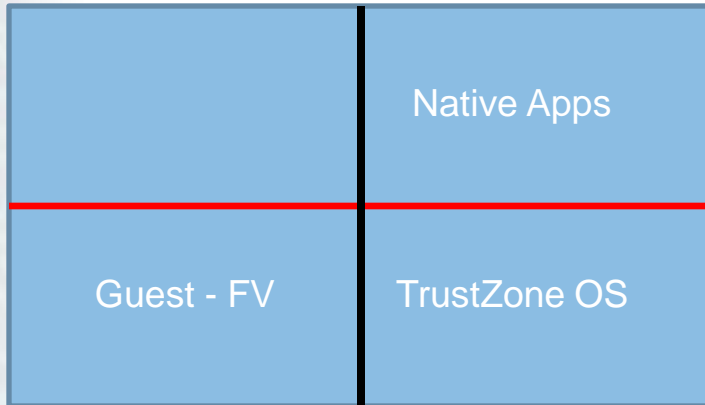
# ARM Secure/Normal State Hypervisor Approaches

Normal State

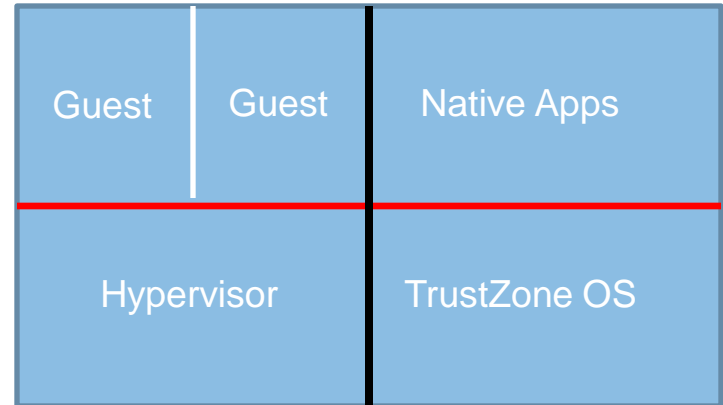
Secure State

User

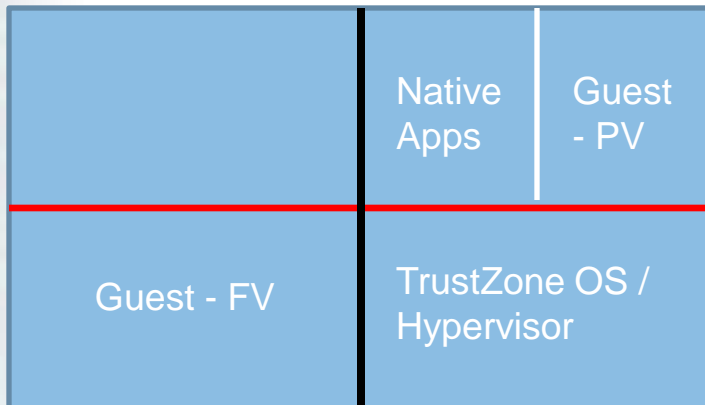
Super



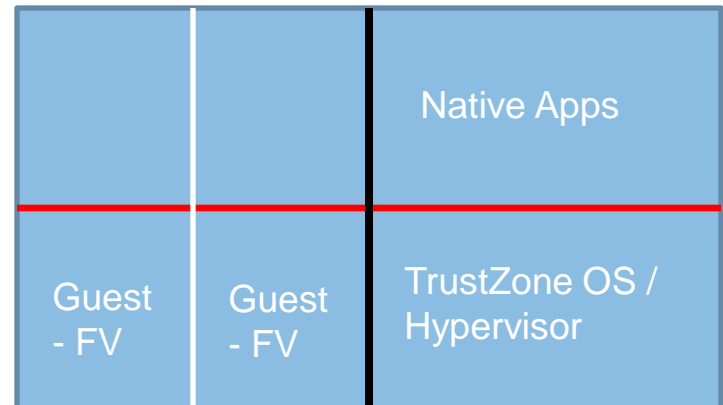
ARM 1176, Cortex A5/8/9



ARM 1176, Cortex A5/8/9/15



ARM 1176, Cortex A5/8/9

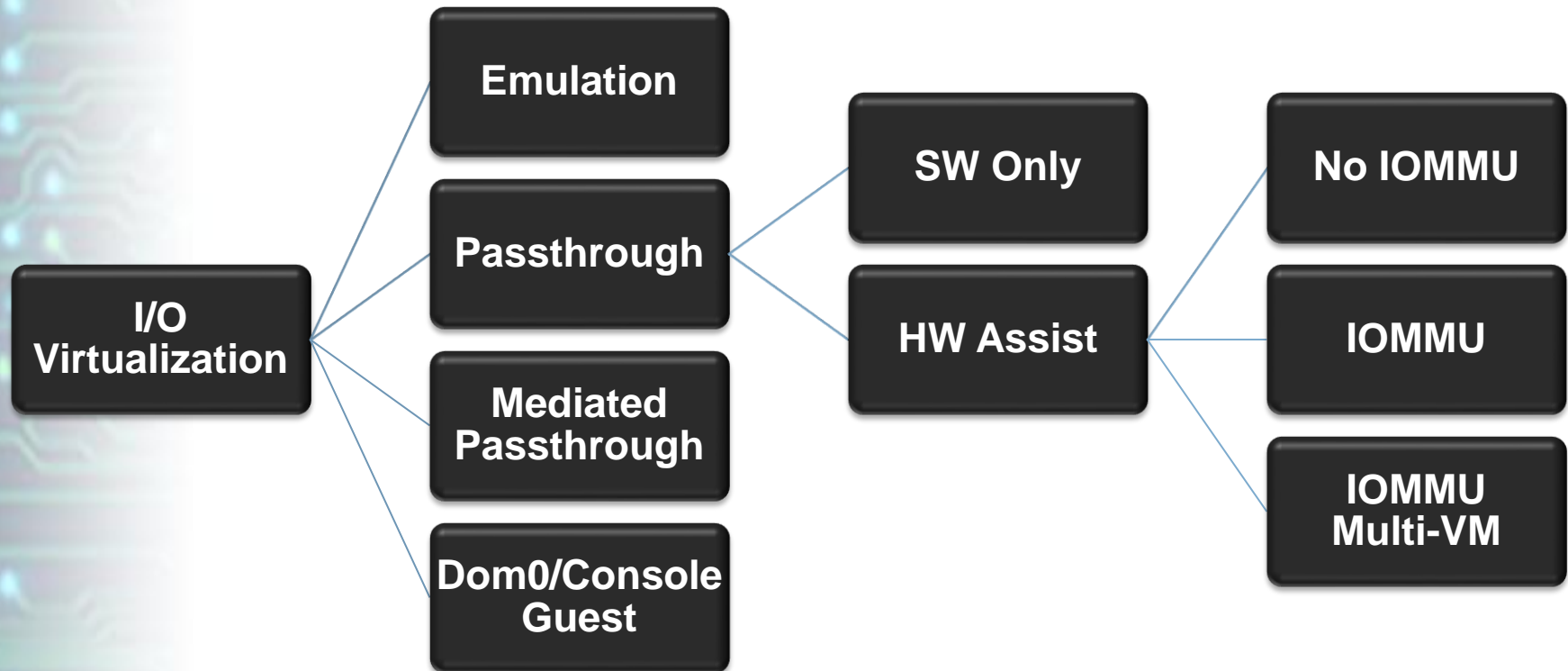


Cortex A15

# ARM Virtualization Extensions

- ❑ Independent of TrustZone
- ❑ Hypervisor mode with exception injection, similar to others
- ❑ Hardware-enforced virtual TLB
  - guest-virtual -> guest-physical -> actual physical
- ❑ IOMMU
- ❑ First core: Cortex A15
  - SoC implementations in 2012

# Type-1 I/O Virtualization Taxonomy



# I/O Virtualization Tradeoffs

	Security and Reliability	Performance	Maintainability	Secure Sharing of I/O
Pass Through, SW Only	Red	Green	Yellow	Red
Pass Through, IOMMU	Yellow	Green	Green	Red
Mediated Pass Through	Green	Yellow	Yellow	Green
Emulated	Green	Red	Yellow	Green
Dom0/Console	Red	Red	Yellow	Red

# In-Vehicle Infotainment

- ❑ Demand for more advanced infotainments growing.
- ❑ Theater-quality audio & video & GPS nav common requirements.
- ❑ Wireless networking & office technologies.
- ❑ Some features must be instant on.
- ❑ High availability.
- ❑ Cost, weight, power and size minimized.

# Embedded and Mobile Use Cases

## ❑ Smartphone/tablet

- Critical components isolated from Android
- IP/Licensing sandbox
- “Bring Your Own”



# Embedded and Mobile Use Cases

- ❑ Military: intelligent munitions system
- ❑ Avionics: electronic flight bag (EFB)
- ❑ Government: secure smartphone
- ❑ Retail: Windows POS + secure transactions
- ❑ Automotive: infotainment + rear-view camera
- ❑ Medical: real-time scan + 3D render + operator
- ❑ Networking: control + data plane
- ❑ Print/imaging: print + remote asset management

# Summary

## ❑ Embedded Virtualization

- Replacing OS abstractions - peripherals, memory, process actors
  - Complete system abstraction: OS actors
- Consolidation for reduced SWaP-C: Linux + RT
- Take advantage of multicore
- Many use cases, innovative platform architectures
  - The Ultimate Open Platform

## ❑ Key Considerations for Embedded – Need:

- Robustness/security
- Real-time
- Embedded virtualization expertise
- Flexibility (e.g. resource partitioning, I/O management)
- Portability of guests and hardware virtualization capabilities
- SDK and ecosystem

## ❑ Questions/slides: [twebb@ghs.com](mailto:twebb@ghs.com)