VIRTUALIZATION AND REAL-TIME SYSTEMS FOR WORK LOAD CONSOLIDATION

Core and Visual Computing Group, Intel®

LEGAL NOTICES AND DISCLAIMERS

WORKLOAD CONSOLIDATION IS A KEY STRATEGIC FOCUS

MANY CUSTOM DEVICES

EXPANDABLE, HIGH PERFORMANCE COMPUTE

LOWER COSTS, INCREASE YIELD AND FLEXIBILITY

INVEST IN WORKLOADS THAT CONSOLIDATE COMPUTE (ATOM → CORE → XEON)

WORKLOAD CONSOLIDATION FOR EDGE COMPUTING

6 Enabling Technology Pillars Powered by IA + Workload Accelerators

Manufacturing Machine

Virtualization | FUSA | Security | Artificial Intelligence | Machine Vision | Real Time

Edge Server
Multi-Function Controller
Edge Gateway

DIGITAL TRANSFORMATION AND WORKLOAD CONSOLIDATION

Technology drives value in businesses in four ways: enhanced connectivity, automation of manual tasks, improved decision making, *and* product or service innovation*. Tools such as big-data analytics, apps, workflow systems, and cloud platforms – all of which enable this value – are too often applied selectively by businesses in narrow pockets of their organization. When used well, digital expands the improvements delivered in one part of an organization across the whole value chain.*

--McKinsey & Company's article, *Finding Your Digital Sweet Spot,8* authors 'Tunde Olanrewaju and Paul Willmott

WHY CONSOLIDATE COMPUTING TASKS?

BUSINESS DRIVERS

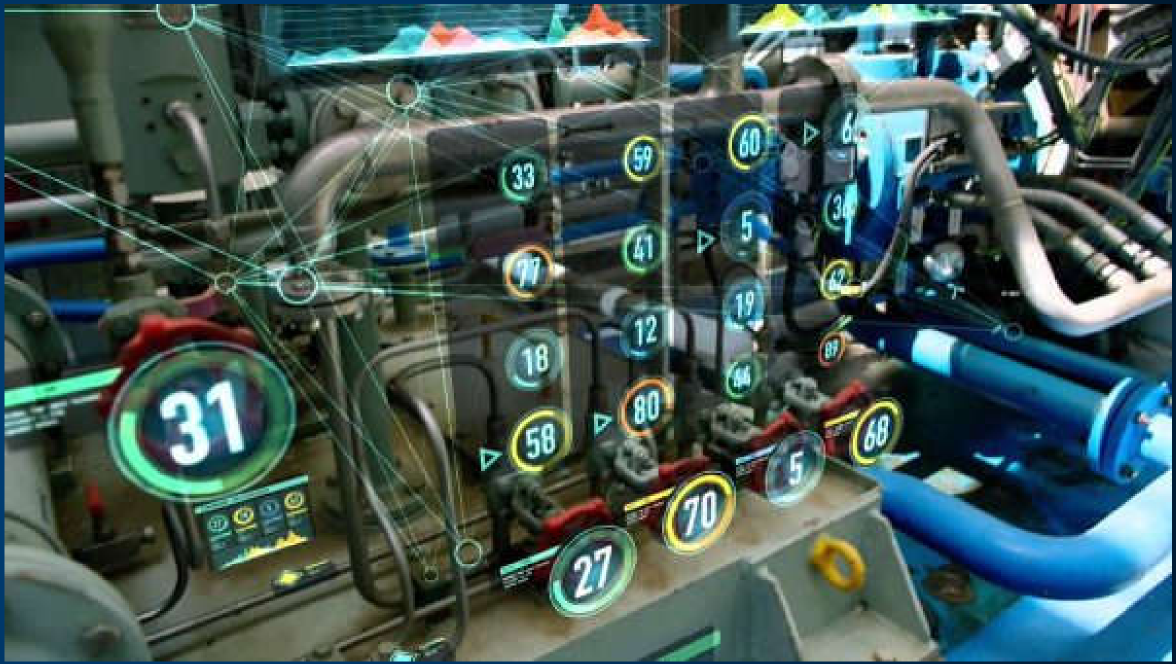
- Lower OPEX/CAPEX
- Faster Time to Revenue
- Aging Workforce
- Increased Security Risk

CUSTOMER DRIVERS

- Lower Downtime
- Increased Output/Yield
- Interoperability for Best of Breed
- Increased Flexibility/Portability

INDUSTRIAL REQUIREMENTS INFLUENCING WORKLOAD CONSOLIDATION

- Worst Case Execution Time
- Bandwidth Capability
- Logical Isolation
- Determinism
- Platform Requirements



VIRTUALIZATION IS A KEY ENABLER FOR WORKLOAD CONSOLIDATION

Static Locked Configuration

Dynamic Configuration

Elastic Configuration and Orchestration

ISOLATION — VIRTUALIZATION SPECTRUM — SCALABILITY

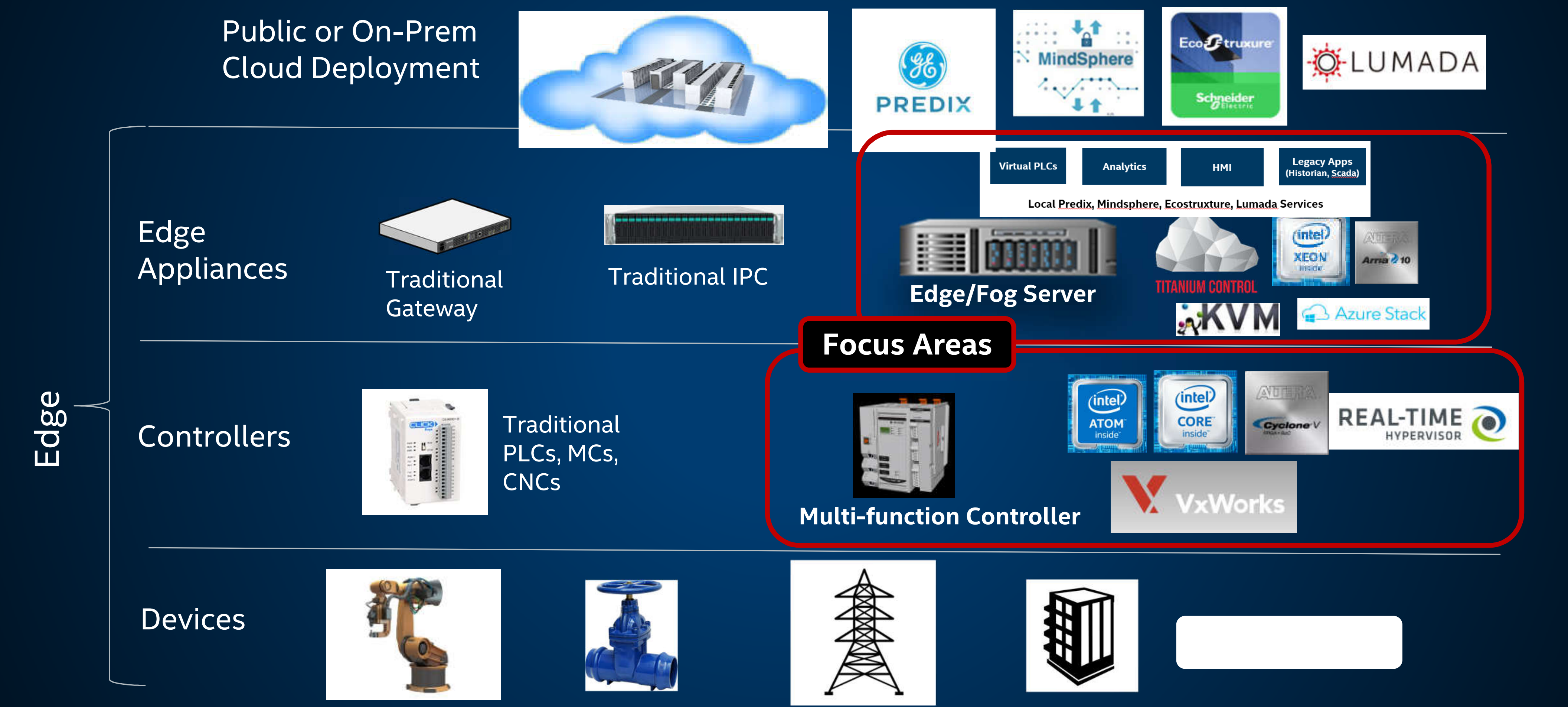
Separation kernels (e.g.VxWorks 653)	Real-Time Hypervisors (e.g. VxWorks HV, RTS, ACRN)	Linux Open Virtualization (e.g. KVM, bhyve)	Container Engines (e.g. Docker)	Cloud-Like Infrastructure at the Edge (e.g. Openstack, Titanium Control, Azure Stack)

VIRTUALIZATION INTERCEPT POINTS

- Workloads
  - Industrial PaaS Offerings
- Virtual PLCs | Analytics | HMI | Legacy Apps
  - GE Predix*, Siemens MindSphere,, Hitachi Lumada*

Software	Orchestration Layer	OpenStack Heat*, Docker/Kubernetes, Appache Mesos*
	OS, Virtualization, Accelerators	Titanium Control, Linux*/KVM, Docker, Azure Stack*, AWS Greengrass*
Hardware	SI Features and Accelerators	FPGA, Security, Graphics, Intel® VTx/d
	Silicon	Intel® Core™/Intel® Xeon® Processors

WHAT TO LOOK FOR: NEW PRODUCT CATEGORIES



WHAT IS INTEL® VIRTUALIZATION TECHNOLOGY

Intel® Virtualization Technology (Intel® VT) is a multigenerational roadmap of increasingly powerful enhancements to Intel Processors, Chipsets and I/O devices. It is a complementary technology to virtualization software products that enhances today's virtualization solutions and lays foundation for future platform virtualization. Intel® VT provides hardware assist to the virtualization software reducing its size and complexity enabling lower cost, more efficient, more powerful virtualization solutions.

QUICK GLANCE OF INTEL® VIRTUALIZATION TECHNOLOGY

CPU	Privileges MMU	VMX/VT-x
I/O	Interrupts DMA Network	VT-d VT-c
GPU	Graphics	GVT-d GVT-s GVT-g

INTEL VIRTUALIZATION PRODUCTS AND TECHNOLOGIES

Intel® VT is a cohesive portfolio of several hardware assist technologies that increase performance and the overall functionality of virtualization software and Intel solutions

Technologies

Intel® VT – x

- CPU Virtualization
- Memory Virtualization

Intel ® VT – d

- I/O Virtualization

Intel ® VT – c

- Virtualization of Network Devices

Other technologies

- Intel Graphics Virtualization Technology[1]

Hardware

Wide Range of Processors

Software

Wide Range of Software*

Supported OSes

Wide Range of Operating Systems*

Solution Benefits

- Higher Privilege Ring: Reprioritized ring eliminates conflicts simplify hypervisor complexity, and improve capability with unmodified OS
- Hardware Based Transitions: Reduces complexity of software transitions
- Hardware Based Memory Protection: Accelerate Transition and ensure reliability of the process

1. Intel GVT is an integrated feature that depends on the processor

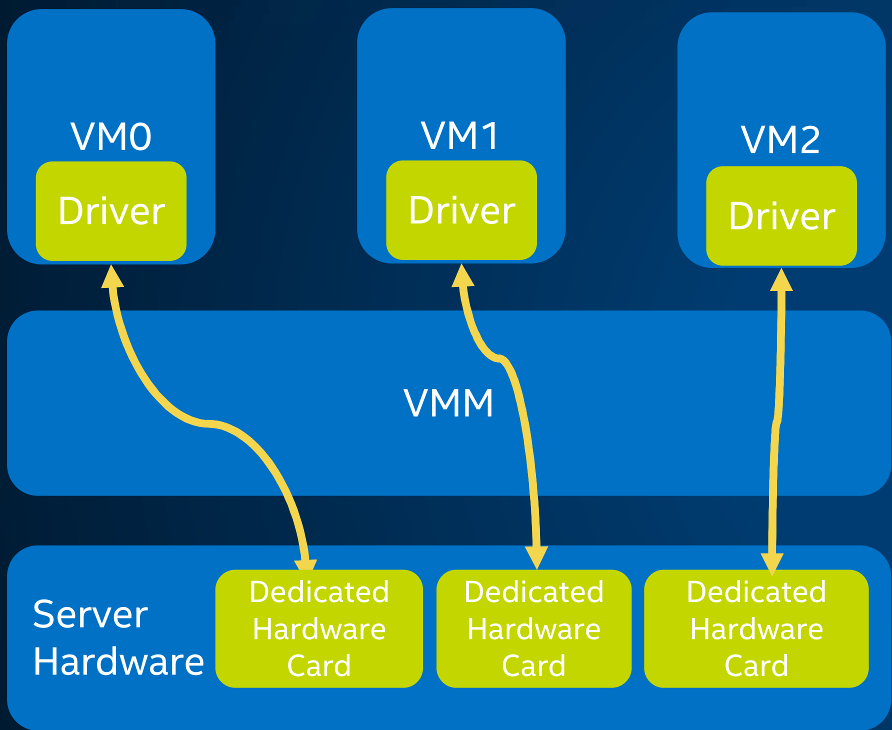
Source: https://www.intel.com/content/www/us/en/virtualization/virtualization-technology/intel-virtualization-technology.html

*Other names and brands may be claimed as the property of others

INTEL® VT-X TECHNOLOGY OVERVIEW

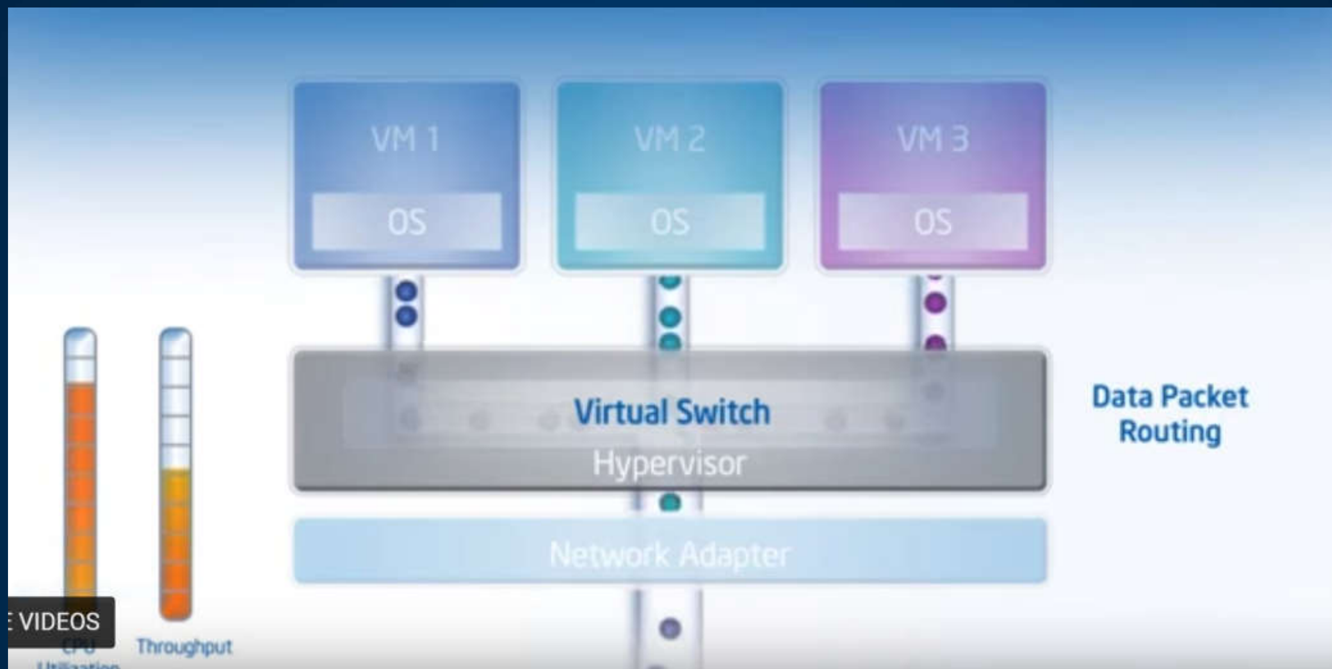
Intel Virtualization Technology Feature and CPU Mapping	
VT-x Base	**CPU virtualization** features enable faithful abstraction of the full prowess of Intel® CPU to a virtual machine (VM)
Intel® VT FlexPriority	optimizes virtualization software efficiency by improving interrupt handling.
Intel® VT FlexMigration	conduct live virtual machine (VM) migration across all Intel® Core™ microarchitecture-based servers.
Extended Page Table (EPT)	allows a VMM to avoid the VM exits associated with page-table virtualization, which is a major source of virtualization overhead without EPT.
Virtual Processor ID (VPID)	permits the CPU to flush only the cache lines associated with a particular VM
Descriptor-Table Exiting	allows a VMM to protect a guest OS from internal attack by preventing relocation of key system data structures
Pause-Loop Exiting	enable detection of spin locks in guest software and avoid lock-holder preemption
Real Mode Support	This feature allows guests to operate in real mode, removing the performance overhead and complexity of an emulator.

INTEL® VT FOR DIRECTED I/O (INTEL® VT-D)



Intel VT-d Feature and Chipset Mapping	
Intel® VT-d Base	hardware support for connecting physical devices to virtual addresses that support direct VM I/O
Interrupt Remapping Support	enables the VMM to isolate interrupts to CPUs assigned to a given VM and to remap/reroute physical I/O device interrupts.
Queued Invalidation Support	Queued-Invalidation enables the VMM to batch digital media translation invalidations.
Address Translation Services Support	allows PCI-e devices to cache the IOTLB entries (used for DMA remapping) of that device directly in the device itself
Support for PCI-SIG/IO Virtualization	

INTEL® VT FOR CONNECTIVITY PROVIDES I/O VIRTUALIZATION



https://www.youtube.com/watch?v=Y-EaX3BBzSc

INTEL GRAPHICS VIRTUALIZATION

Efficiency in today's world often implies the use of cloud computing, and today's cloud faces a growing share of media-rich workloads. While this impending reality has often presented a steep challenge, graphics virtualization technologies have emerged in response, to efficiently manage these workloads.

- Intel offers a full suite of graphics virtualization technologies, known as Intel® Graphics Virtualization Technology (Intel® GVT), that offer different approaches with varying levels of performance, capabilities and sharing to best meet the needs of a wide range of developers.
- *Intel® Graphics Virtualization Technology –d (Intel® GVT –d)*: vDGA: virtual dedicated graphics acceleration (one VM to one physical GPU)
- *Intel® Graphics Virtualization Technology –s (Intel® GVT -s)*: vSGA: virtual shared graphics acceleration (multiple VMs to one physical GPU)
- *Intel® Graphics Virtualization Technology –g (Intel® GVT -g)*: vGPU: virtual graphics processing unit (multiple VMs to one physical GPU)

SUMMARY OF INTEL® VIRTUALIZATION TECHNOLOGY

HYPERVISORS

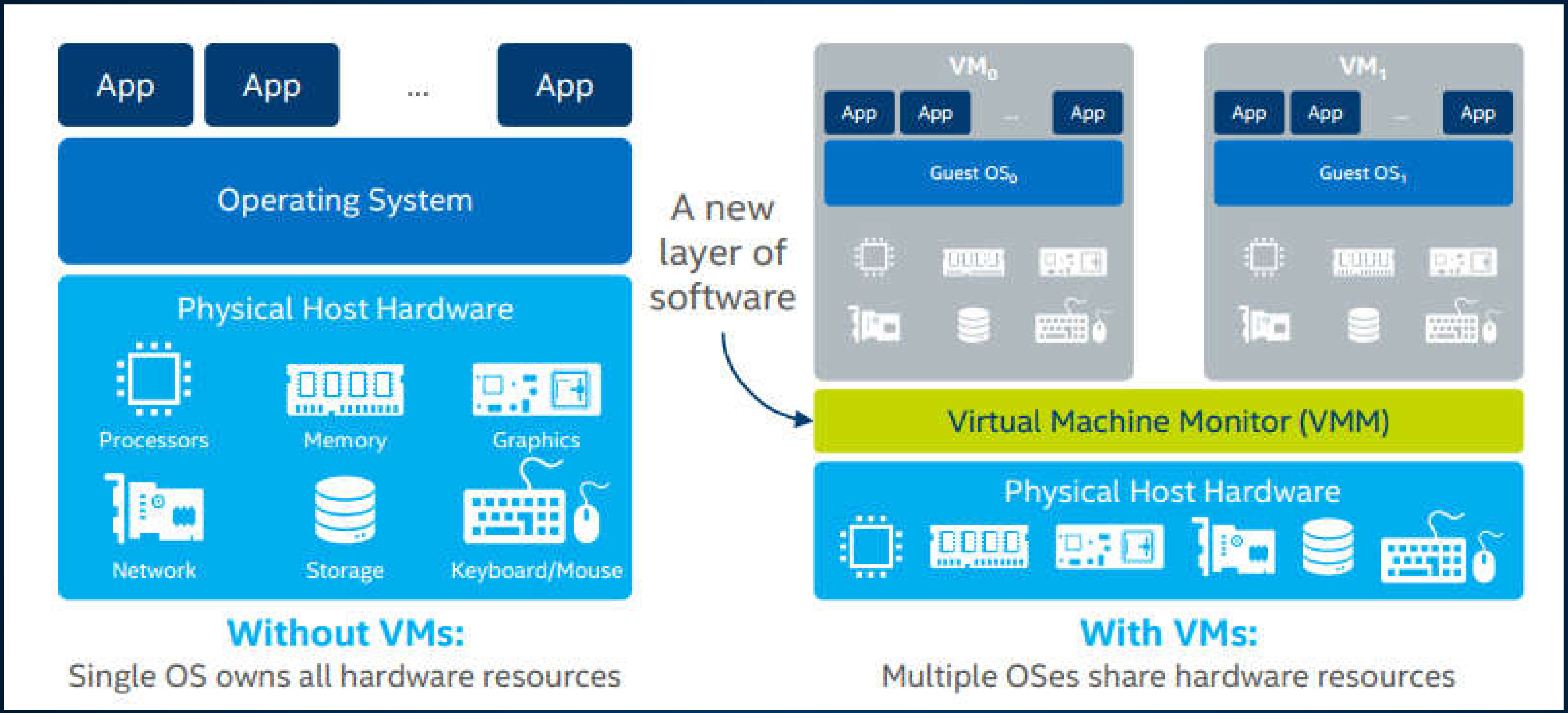
HARD VS. SOFT REAL-TIME REQUIREMENTS

The primary difference between hard and software real-time systems is the consequences of missing a scheduling deadline.

- Hard Real-Time: scheduling deadlines must be met every single time. Missing the deadline means the system has failed, possibly with catastrophic consequences.
  - Robotic assembly line that require a high degree of timing accuracy
  - Software for dropping control rods in a nuclear power plant

- Soft Real-Time: can tolerate missing a deadline occasionally, if an average latency is maintained.
  - A system reporting on the current activity of the assembly line will not have catastrophic results if the information is slightly delayed

HYPERVISOR ARCHITECTURE



	Type 1 Hypervisor (Bare Metal or Native)	Type 2 Hypervisor (Hosted)
Installation	Works directly on the hardware of the host and can monitor operating systems that run above the hypervisor	Installed on an operating system and supports other operating systems above it
OS	Completely independent of the OS	Completely dependent on the host OS for its operations
Memory	Small: its main task is sharing and managing hardware resources between different operating systems	Bigger memory footprint: while having a base OS allows better specification of policies, any problems in the base OS affect the entire system even if the hypervisor running above the base OS is secure
Advantage	Any problems in one VM or guest OS do not impact the OS running on the hypervisor Allows for much better real-time (RT) turnaround	In a scenario where a customer has a legacy OS running a proprietary embedded application but wants to co-host a newer application that the legacy OS cannot support, one can host a newer OS that supports the newer application in the legacy OS environment

Typical Layers

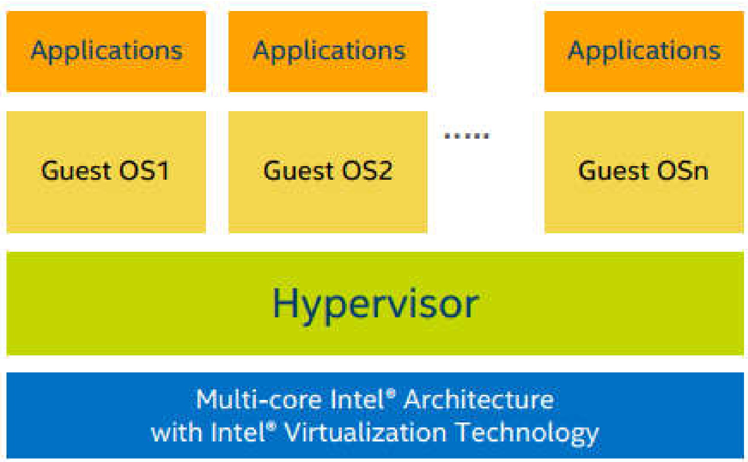


Figure 5. Different Layers typical for a Type 1 Hypervisor Model

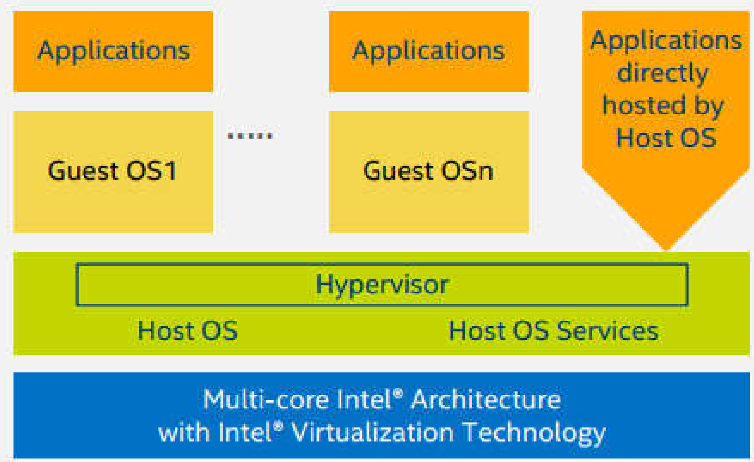
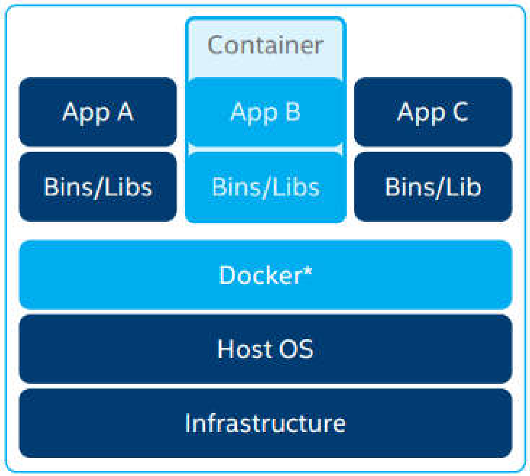
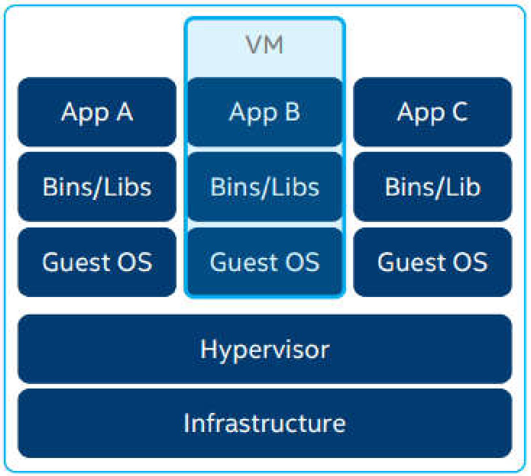


Figure 6. Different Layers typical for a Type 2 Hypervisor Model

VIRTUALIZATION VS. CONTAINERIZATION





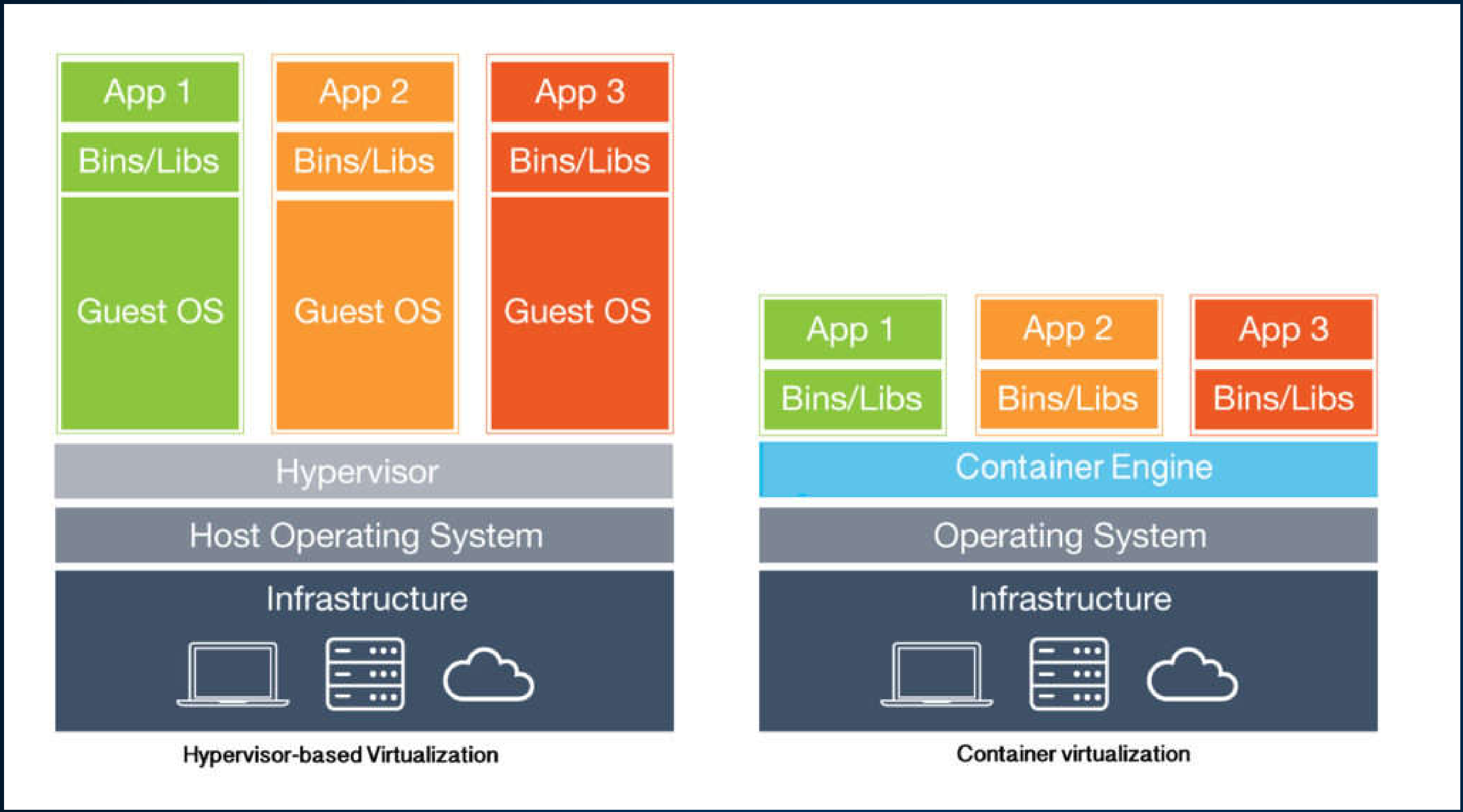
Containers

Containers are an abstraction at the app layer that packages code and dependencies together. Multiple containers can run on the same machine and share the OS kernel with other containers, each running as isolated processes in user space. Containers take up less space than VMs (container images are typically tens of MBs in size) and start instantly.

Virtual Machines

Virtual machines (VMs) are an abstraction of physical hardware turning one server into many servers. The hypervisor allows multiple VMs to run on a single machine. Each VM includes a full copy of an operating system, one or more apps, necessary binaries and libraries – taking up tens of GBs. VMs can also be slow to boot

VIRTUAL MACHINES VS. CONTAINERS



TITANIUM CONTROL

Wind River® Titanium Control is the future of critical infrastructure. Keep your systems running, keep them current, and keep your costs down.

2017 STEVIE® BRONZE WINNER
AMERICAN BUSINESS AWARDS

Product Overview

IA FEATURES LEVERAGED BY TITANIUM CONTROL

Platform Feature	Description	Technology Baseline	Use Cases	Titanium Control Implementation	Benefits
Vt-X	Accelerates virtual machines to near bare metal performance	Xeon / XeonD	Near native virtualized CPU performance	Performance enhancement of VMs, live migration from one Intel CPU generation to another	Performance and scalability
Vt-D	Enables physical NICs and/or GPUs to be mapped directly to virtual machine	Xeon/ XeonD	Native I/O performance	PCI Passthrough and SR-IOV support	Performance and salability
AVX-512	Enables high performance vector workloads	Xeon Skylake Xeon Scalable Processor	Telecom, AI, high performance storage, encryption and compression	Enhanced KVM performance, guest AVX-512 support	Performance and scalability
Trusted Execution Technology	Used to attest system authenticity and state	TPM 2.0	Secure boot and verified system state	Secure boot, TPM 2.0 storage of communication keys, vTPM 2.0 support in guests.	Security
AES-NI	Accelerates encryption/decryption	Xeon Westmere +	Full disk encryption and faster communications	Linux encryption performance enhancements	Security
UEFI Boot	Used for secure booting	UEFI Spec 2.6+	Secure booting and faster boot	Fast boot, secure boot	Security

IA FEATURES LEVERAGED BY TITANIUM CONTROL #2

Platform Feature	Description	Technology Baseline	Use Cases	Titanium Control Implementation	Benefits
DPDK	Library to accelerate networking path	Intel DPDK	High speed VM-to-VM networking	Optimized DPDK libraries	Performance and scalability
QuickAssist	Hardware-based compression and encryption	Coleto Creek, VT-d	Exposing QuickAssist engine to VMs and virtualization of QuickAssist across VMs	Support PCI passthrough and SR-IOV access for VMs to QuickAssist accelerators	Security
Enhanced Platform Awareness (EPA)	Set of enabling features that take full advantage of Intel Architecture through OpenStack		Performance / determinism controls such as core pinning, NUMA awareness / controls, hyperthreading awareness / controls, CPU model selection	Suite of features that provide fine grained control for VMs. Can specify core pinning, NUMA affinity to vSwitch and NICs, split NUMA VMs, hyperthreading isolate or require, select CPU model to enable / disable CPU capabilities / instruction sets, huge page sizes.	Performance and scalability

MULTI-FUNCTION CONTROLLER WITH VXWORKS

ROCKWELL COMPACT LOGIX 5480 CONTROLLER

https://www.youtube.com/watch?v=TovqAiZcCCk

Windows

Windows App

Windows App

Windows App

Logix Control Engine

Realtime Hypervisor (VxWorks)

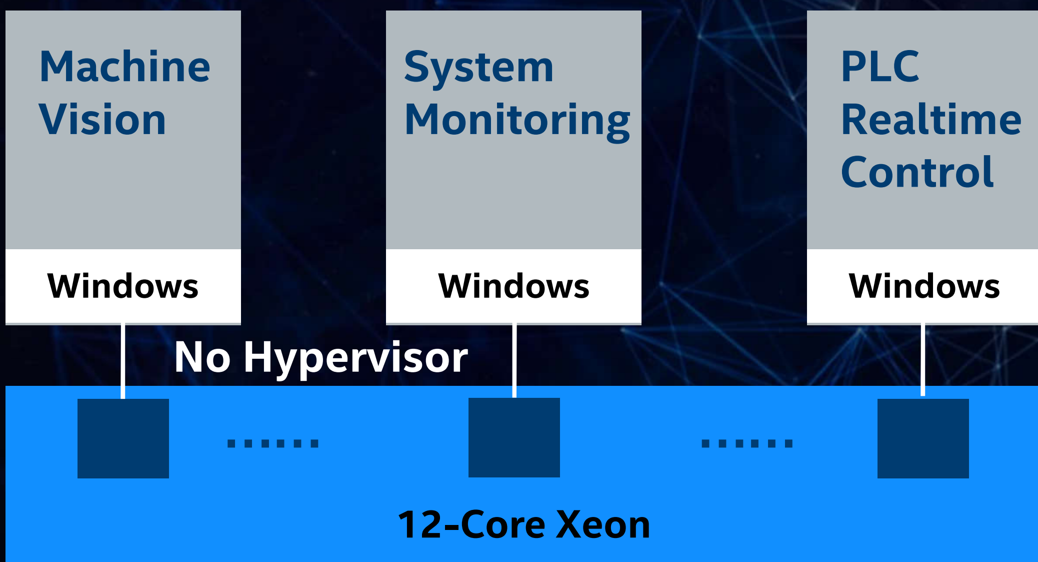
Core i7

Opportunity	Problems Solved
Core CPU with real-time Hypervisor	▪ Ability to run Windows Applications alongside real-time Control Engine ▪ Leveraging existing PLC install base and extending value/revenue stream of assets

WORKLOAD CONSOLIDATION WITHOUT VIRTUALIZATION

https://www.youtube.com/watch?v=miEOxPZ9IIA

BECKHOFF CX2072 CONTROLLER



Opportunity	Problems Solved
High-end multi core Xeon CPUs	▪ Maximum performance by direct assignment of workloads to cores (no Hypervisor) ▪ Differentiation over competitor products ▪ Workloads assigned statically from Twincat environment

SUMMARY

- Workload Consolidation trends are driving down capital equipment and maintenance prices while increasing factory flexibility and efficiency.
- Intel® Virtualization Technologies including Intel® VT-x, VT-d, VT-c and VT-g allow multiple workloads to be consolidated into a single machine.
- Intel® Virtualization Technology is being adopted by real-time hypervisors, operating systems and applications enabling real-time workload to be consolidated.
- Intel supports and Industrial Ecosystem of Commercial and Open Source partners.

RESOURCES

- Intel® Virtualization Technology (Intel® VT)
- Intel® Virtualization Technology for Directed I/O (VT-d): Enhancing Intel platforms for efficient virtualization of I/O devices
- PCI-SIG SR-IOV Primer
- Intel® Data Direct I/O Technology
- Data Plane Development Kit (DPDK)
- Does My Processor Support Intel® Virtualization Technology?

intel®