Advances using Intel® Processor Technology
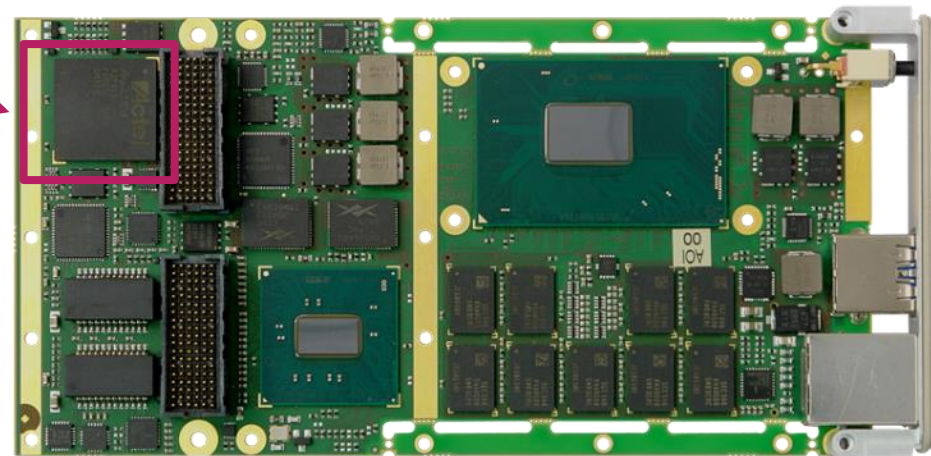
Security

- **Has a higher profile but…….**
- **Still many areas of improvement needed to:**
  - Prevent unauthorized use of secure equipment
  - Prevent unauthorized access to sensitive data

ENABLING HIGH SECURITY SOLUTIONS

INSECURE BOOT
ROGUE SOFTWARE
ILLICIT MODIFICATION OF NON-VOLATILE MEMORY
BOARD LEVEL
SECURITY
SYSTEM CONFIGURATION TAMPERING
LOW-LEVEL FIRMWARE HACK
ILLEGAL ACCESS OF CLASSIFIED DATA

CONCURRENT TECHNOLOGIES

Security Options

- **We have experience supplying products to the defence markets**
- **Customer selects measures to protect against:**
  - physical intrusion
  - **booting from non-secure sources**
  - accessing classified data
  - retrieving sensitive Intellectual Property
  - modifying non-volatile memory
  - **executing non-trusted software**
  - unauthorized modification of system configuration
  - **bypassing low level firmware**
  - reverse engineering
- **Delivered using standard and custom firmware/hardware**

CONCURRENT TECHNOLOGIES

Security on Future Intel® AdvancedMCs

- **We will provide enhanced security capabilities**
- **Security requires (significant) user effort**
- **Some questions you should ask:**
  - Where are the weak spots in my solution?
  - What aspects of security are important?
  - How much should I share?

> Is security something you can ignore?

Storage – Interface speeds

Dramatic increase in local storage interface speeds
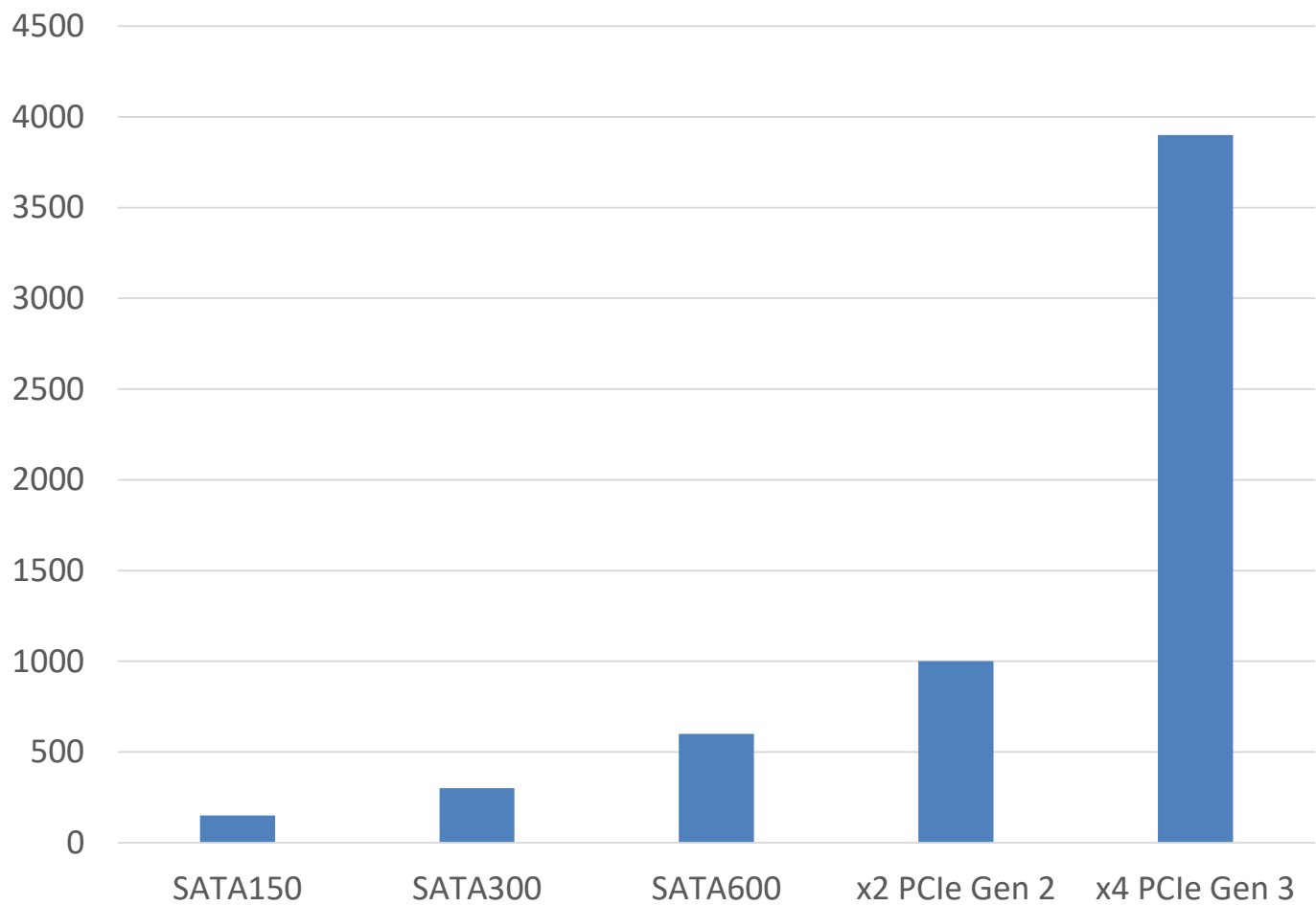
Storage Devices and Protocols

- **NVMe protocol - leverages the low latency and parallelism of PCI Express to enable performance enhancements over AHCI**
- **Linux, Windows and VMware support**

Intel® SSD Pro 6000p Series
(1.0TB, M.2 80mm PCIe 3.0 x4, 3D1, TLC)

42, 60 or 80mm long

22mm wide

Specifications ^
- Essentials
- Performance
- Reliability
- Package Specifications
- Advanced Technologies

Product Images ˅

Ordering / sSpecs / Steppings ˅

Download Drivers ˅

Specifications

Essentials

Capacity	1.02 TB
Status	Launched
Launch Date	Q3'16
Recommended Customer Price	$364.00

Performance

Sequential Read (up to)	1800 MB/s
Sequential Write (up to)	560 MB/s
Random Read (8GB Span) (up to)	155000 IOPS
Random Write (8GB Span) (up to)	128000 IOPS

Future Double AdvancedMC

- **Replace single 2.5-inch drive with 2 x M.2 modules**
  - Intel Rapid Storage Technologies support RAID modes 0,1,5 and 10
  - High storage capacity
 - Dramatic increase in performance

CONCURRENT
TECHNOLOGIES
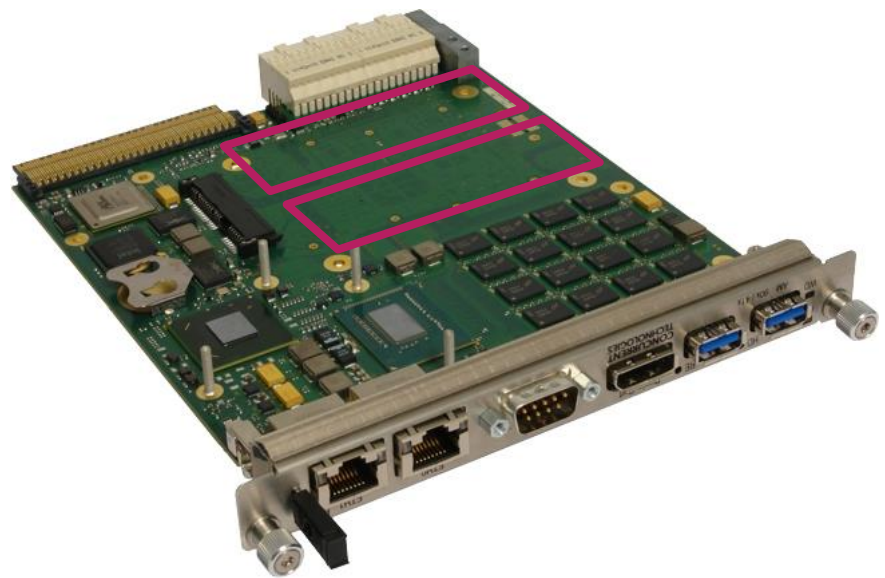
Operating System Support

**Future Intel processors are likely to be available with 64-bit OS support only**

| Board Generation	Linux	Windows	Other
AM 90x/x1x	RHEL 6.4 32/64-bit Ubuntu 13.04 32/64-bit	Windows 7 32/64-bit Windows 8.1 32/64-bit Windows Server 2008 SP1 32/64-bit Windows Server 2012 32/64 bit	VxWorks 6.9.4.6 32/64-bit QNX 6.5.0 SP1
Future AdvancedMC	RHEL 7.2 64-bit Ubuntu 16.04 64-bit	Windows 10 64-bit	VxWorks 7 64-bit

Virtualization

- **Still not widely used in embedded applications**
- **Provides a safe, encapsulated way to add software**
- **We can provide some unbiased advice on using:**
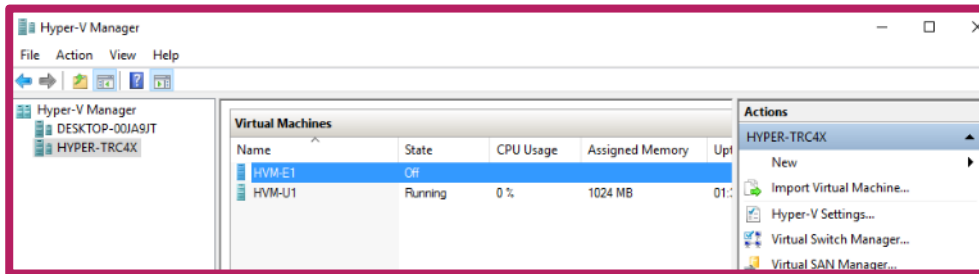
Microsoft Hyper-V
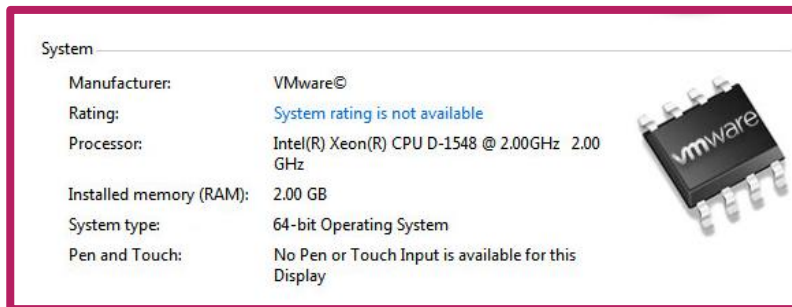
VMware ESXi 6.0
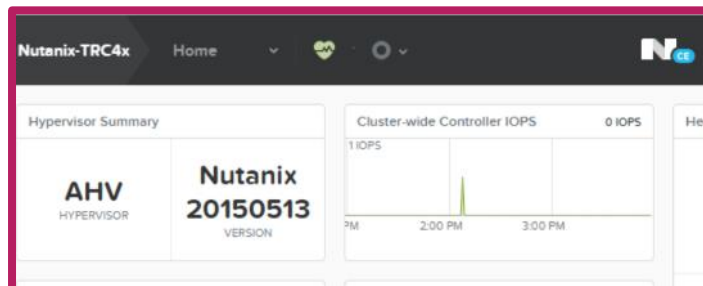
Nutanix HCIS

Thank you

Season's Greetings!

Concurrent Technologies – the source for modular, open standards based Intel® processor boards for long-life embedded applications