IDF2011
INTEL DEVELOPER FORUM

Designing for Next Generation Best-In-Class Platform Responsiveness

Pete Dice
Lead BIOS Architect
Intel Chipset Components Group

EFIS004

Sponsors of Tomorrow.™ intel

Please Fill out the Online Session Evaluation Form

Be entered to win fabulous prizes everyday!

Winners will be announced at 6pm (Day 1/2) and 3:30pm (Day 3)

You will receive an email prior to the end of this session.

Agenda

- Responsiveness Introduction
- 2012 Technology Improvements in UEFI
  - Active Resume BIOS Update
  - Intel® Rapid Start Technology
  - Intel® Smart Response Technology
  - Fast USB Enumeration
- Building in Responsiveness
- Summary

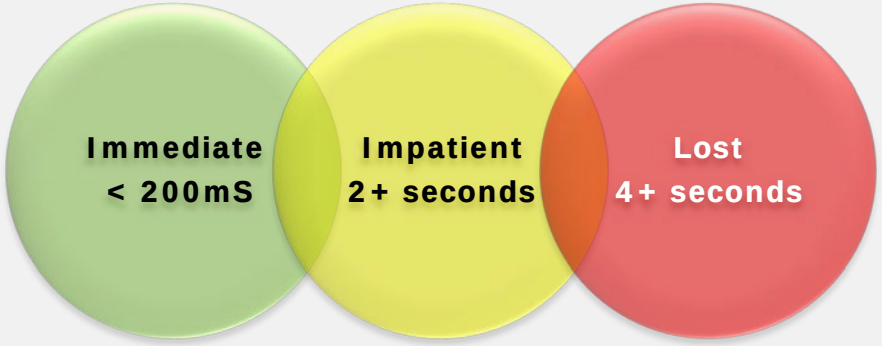
Responsiveness in BIOS?

- Traditionally Slow boot times
- Longer-than-wanted resume times
- ACPI S-State vs. Latency Trade-offs
- Limiting usage models
  - Stale Web content, Specific Target OS
- Potential for customization
  - Scaling the embedded point-solution up/out
  - Unmanageable code/source

Major Improvements Possible with UEFI

The Human Factor

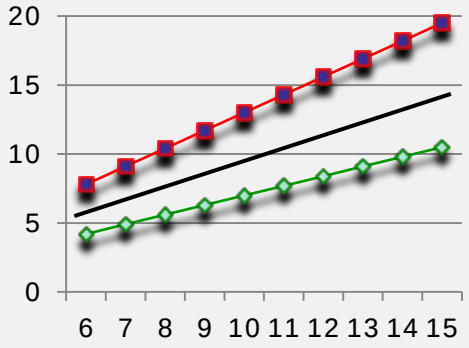
Our Brain's Perception



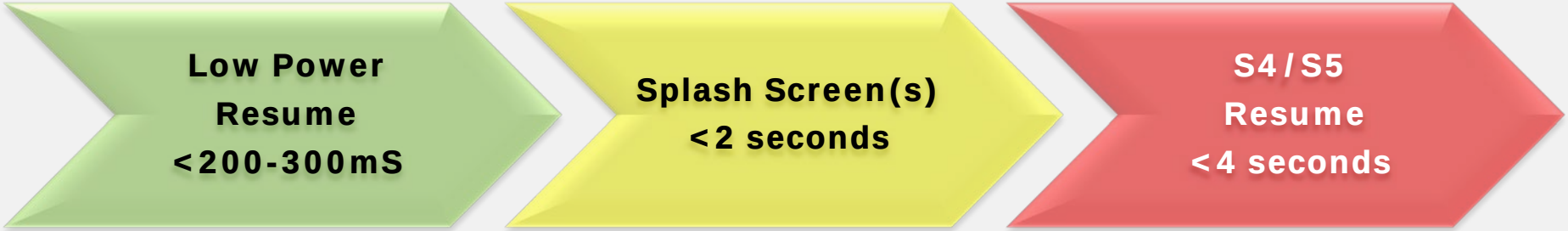
Miller 1968

Hard to Detect Variations

- 75% of people cannot detect change of +/- 8% between 2s and 4s
- From 0.6 to 0.8 seconds was 10% variation
- From 6 to 30 seconds, a 20-30% variation

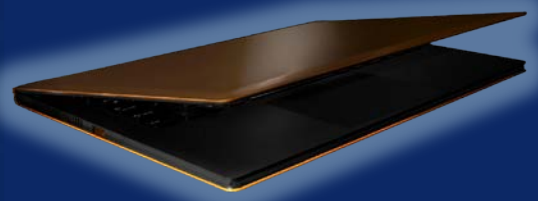


What does this mean to developers?



Excellent, Good, Fair

Commonality across Client Segments

Tablets	*Laptops*	*Desktops*
Thin and Light		
Low Power		
Energy Efficient		
Equally Responsive		
		

Achieve Responsiveness with UEFI

IDF2011
INTEL DEVELOPER FORUM

Agenda

- Responsiveness Introduction
- **2012 Technology Improvements in UEFI**
  - **Active Resume BIOS Update**
  - Intel® Rapid Start Technology
  - Intel® Smart Response Technology
  - Fast USB Enumeration
- Building in Responsiveness
- Summary

Active Resume BIOS Update

Usage & Benefits

System Sleep, S3

System On, S0

Power Sequence | BIOS Resume | OS Resume | Panel Timing

Benefits

- Faster S3
- Shared SEC/PEI with S4/S5 boot
- Intel® Rapid Start Technology
- Intel® Smart Connect Technology

Applies to

- Any Intel® Core CPU, Intel® 7 Series CS
- CPU Core Integrated Graphics
- UEFI BIOS

Intel 2010 Customer Reference Board - S3 Resume Experiments

GUID Description	Execution Time (mS)
Core PEI	4
CMOS Manager PEI	2
WDT App PEI	1
SB PEI	21
PCH SMBUS Arp Disabled	5
TCG PEI	1
Over clocking Init	1
NB PEI	5
PCH init PEI	2
TXT PEI	1
Memory Init	12
CPU PEI Before Mem	3
CPU PEI	**204**
Total time to wake vector*	**~313**

Total of ~200mS spent on CPU PEI init; 65% of the total BIOS S3 resume time

GUID Description	Execution Time (mS)
GetS3ResumeVariable	3
Find Microcode then copy to memory	3
StartAllAps	45
DisableAllNem	3
LoadMicrocodeOnCpus	51
EnableCacheOnCpus	84
Total	**~204**

* - Certain SEC routines and PEI dispatcher and other overhead may not be accounted for in table above. Dozen+ steps took less than 1mS and registered 0mS .

S3 Optimization Prototype Results

	S3 BIOS Execution Time
Starting Point	313 mS
Preliminary effort	200 mS
Final Results	**85 mS***

Preliminary savings 100mS

- Moved from 33MHz to 50MHz SPI
- House Keeping per latest BIOS specs
  - Manage APs in batch mode
  - Loading MUs in parallel
  - Enabling Caches in parallel
  - Any semaphores should be 128B aligned

Final Results: <100mS

- Turn on Prefetching before uCode load
- Do not detect TPM presence more than once
- Remove unused code paths
- Shadow Setup menu variable in block read
- Use smarter AP initialization loops
- Cache CPU PEI in memory before execution

* - based on Intel CRB with specific configuration without a TPM

Active Resume BIOS provides a starting point

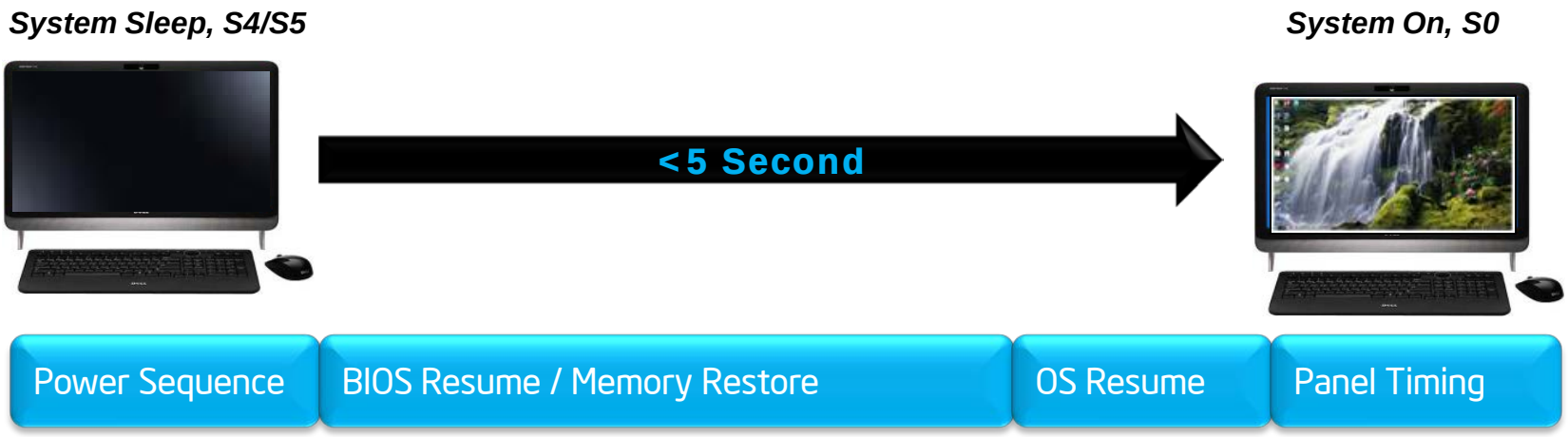
- Work with your IBV to achieve optimized S3 path
- Request this feature from your motherboard vendor
- Talk to your Graphics Vendor about restart of drivers
- Talk to your OS vendor about Resume time, Panel Timing request
- Talk to your Panel Vendor about minimizing backlight timings

Agenda

- Responsiveness Introduction
- **2012 Technology Improvements in UEFI**
  - Active Resume BIOS Update
  - **Intel® Rapid Start Technology**
  - Intel® Smart Response Technology
  - Fast USB Enumeration
- Building in Responsiveness
- Summary

Intel® Rapid Start Technology

Usage & Benefits



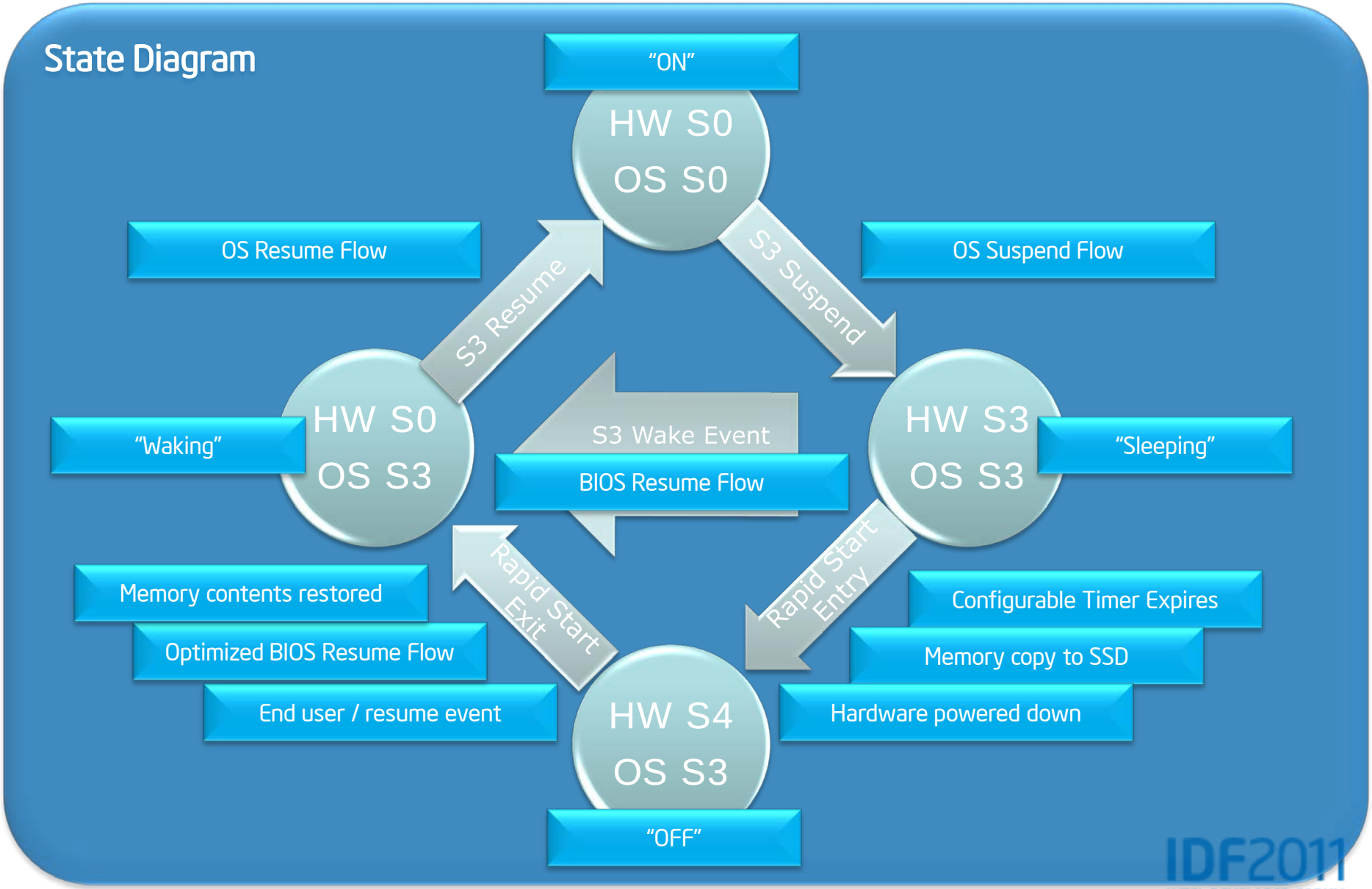
Benefits

- Replaces OS hibernate function with BIOS function
- HW Powers down to S5 state
- OS resumes back as if from S3

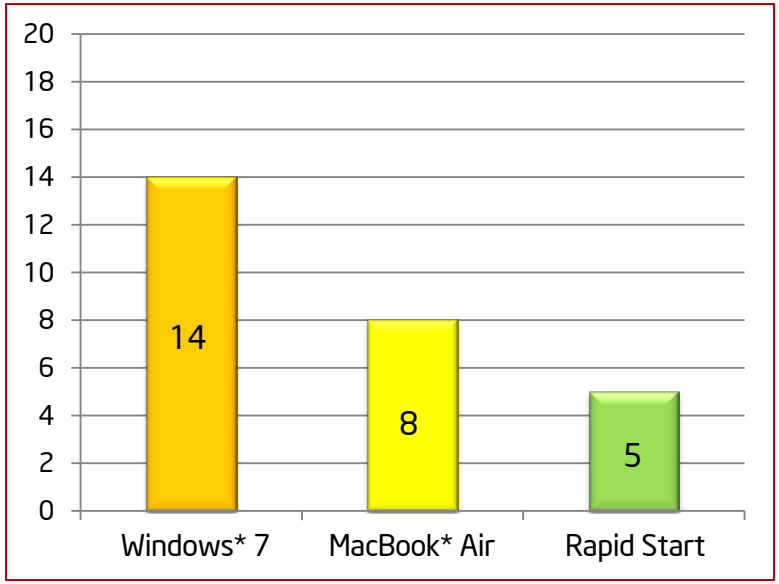
Requirements

- UEFI BIOS with Intel UEFI Ref Code
- Private SSD partition equal to memory size
- Special Partition Table entry into GPT
- Additional ACPI hooks and security precautions for SSD/SMRAM.

Intel® Rapid Start Technology Overview

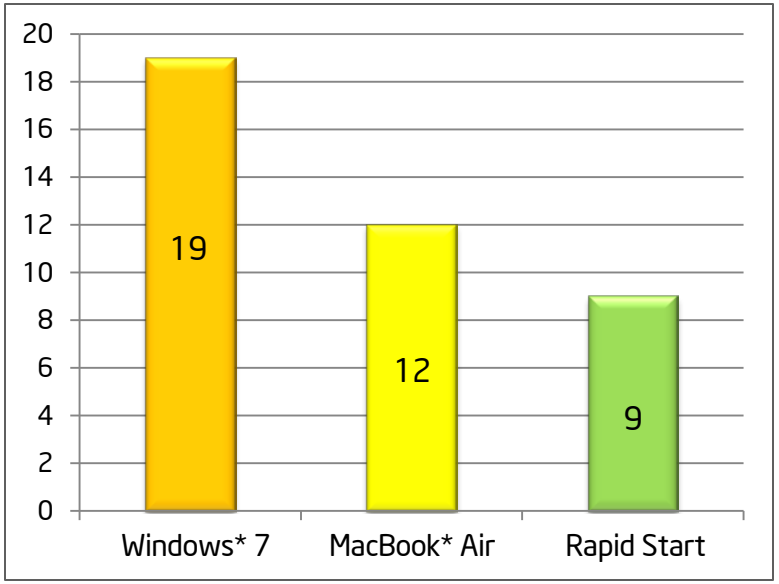


S0 Resume - Intel® Rapid Start Technology compared to Windows* 7 and MacBook* Air



Idle

1.6 to 2.8 times Faster



Loaded

1.3 to 2.1 times Faster

Notes/Source:

All data is based on SATA2 SSD. Performance may vary per device generation and current workload.

Windows* 7 – Intel reference platform, Windows*7 OS, Intel® Core™ i5 CPU, 4GB of memory, Intel® Series 6 Chipset. OS hibernate resume

MacBook* Air - MC505LL/A 11", 4 GB 1066 MHz DDR3, 1.4GHz Core™ 2 Duo, after sleeping for greater than 70 minutes

Rapid Start – Win7 Hardware with Intel® Rapid Start Technology applied

Intel® Rapid Start Technology Summary

- Improves Existing OS boot time experience
- Saves power and battery life over S3
- Performance can vary with:
  - SSD data-readiness time
  - SATA generation of drive/controller
  - OS Application Load
- Works with and Complements:
  - Active Resume BIOS Update
  - Intel® Smart Connect Technology
  - Intel® Smart Response Technology

Contact your BIOS vendor
UEFI Reference code available under NDA through Intel Field

Agenda

- Responsiveness Introduction
- **2012 Technology Improvements in UEFI**
  - Active Resume BIOS Update
  - Intel® Rapid Start Technology
  - **Intel® Smart Response Technology**
  - Fast USB Enumeration
- Building in Responsiveness
- Summary

Intel® Smart Response Technology

- Combines capacity of HDD with speed of an SSD
- Two storage devices look like a single device to the OS and user
- Uses standard (SATA) ports for both drives.

Benefits

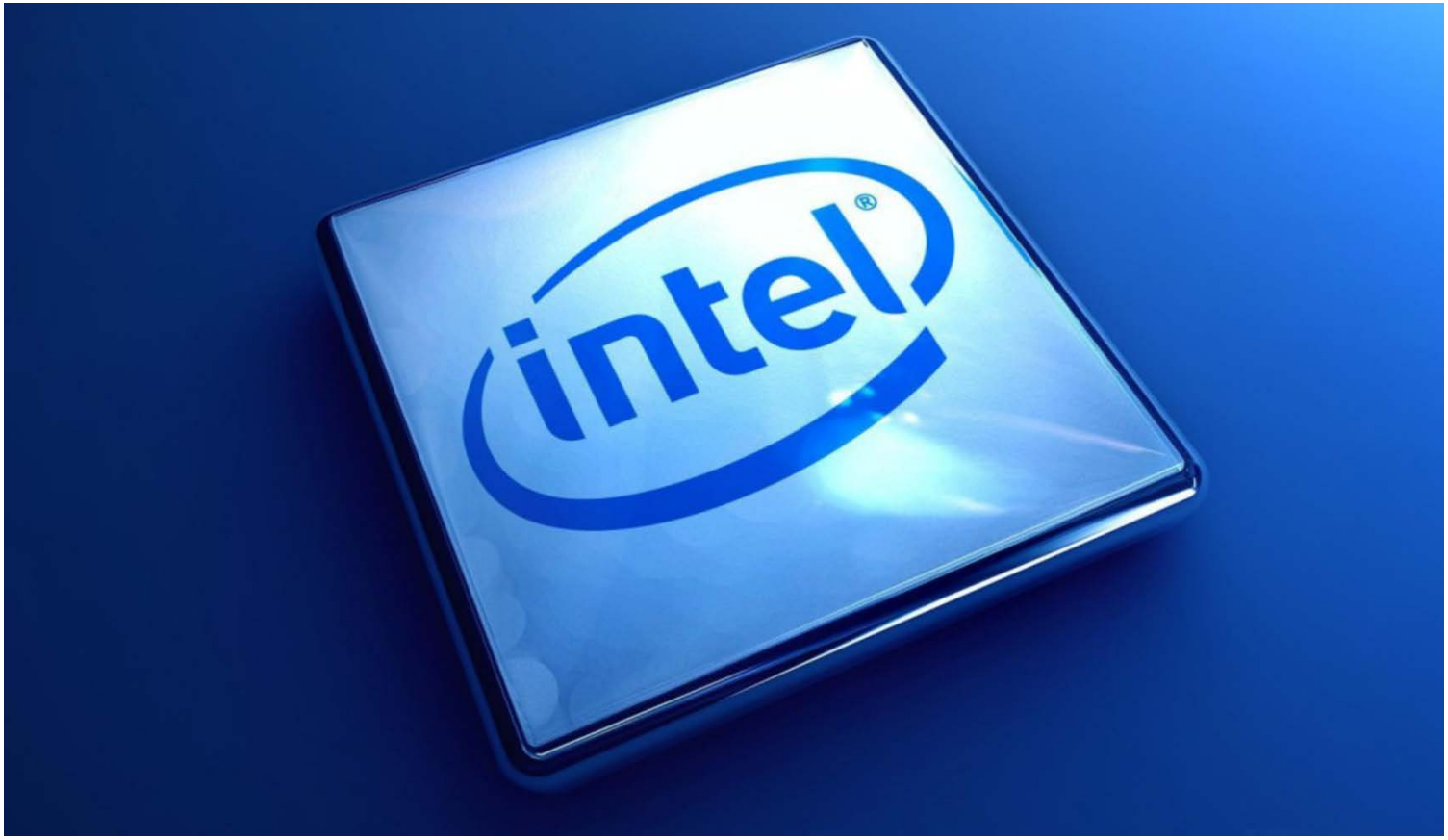
- High Performance - System Boots and Applications load with SSD-like performance
- Less Cost – than large capacity SSD
- Large Capacity - equal traditional HDD
- Lower Power - avoids spinning up HDD as often

Requirements

- Intel® 6 & 7 Series Chipset supporting RAID (i.e. H77, Z77, Q77, Z68)
- Both SSD and HDD installed and active
- SATA-connected SSD of at least 20GB
- mSATA port is optional but provides small space for SSD upgrade option
- Requires the RAID Legacy Option ROM or UEFI driver to be supported in BIOS

Intel® Smart Response Technology

Demo



Intel® Smart Response Technology Summary

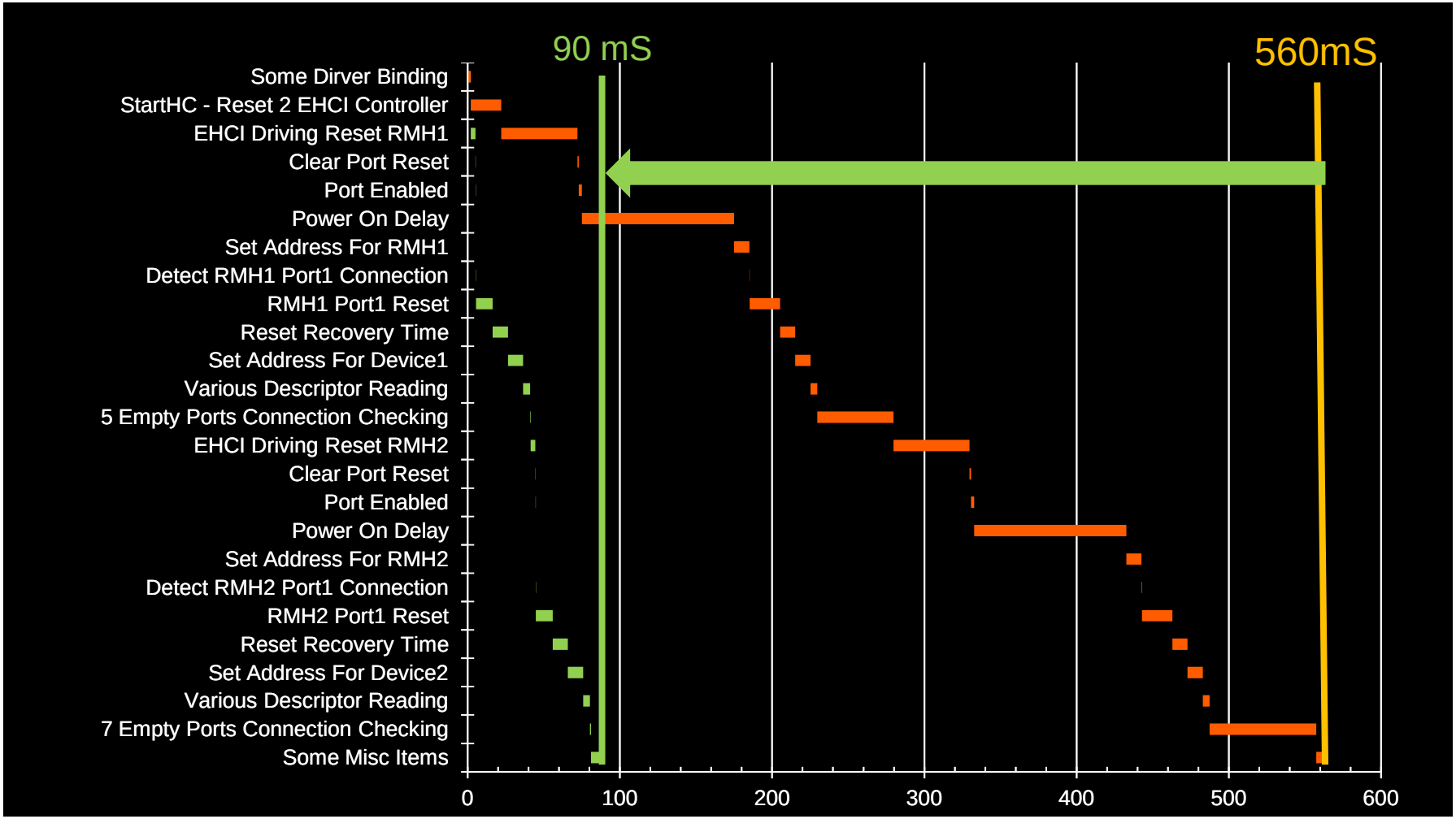
- Improves Existing OS boot time and runtime experience
- Saves power by using primarily SSD and leaving HDD spun down
- Performance can vary with:
  - SATA generation of drive/controller
- Works with and Complements:
  - Intel® Smart Connect Technology
  - Intel® Rapid Start Technology

Intel® 6 & 7 Series Chipsets with support this capability
(ie. H77, Z77, Q77, Z68)

Agenda

- Responsiveness Introduction
- **2012 Technology Improvements in UEFI**
  - Active Resume BIOS Update
  - Intel® Rapid Start Technology
  - Intel® Smart Response Technology
  - **Fast USB Enumeration**
- Building in Responsiveness
- Summary

USB2 Enumeration Timing*



2 USB HID Devices <100mS

- Based on Intel reference platform, Intel® Core™ i5 processor with Intel® Series 6 chipset.
- Performance varies per number or type of USB devices

How?

Optimizations	Savings (ms)	Notes
Skip Power On delay	200	RMH ports are powered from the motherboard. No power on delay needed. 100mS per RMH saved.
Optimal RMH Ports Reset handling	118.8	Only perform reset if device connected.
EHCI driving shorter reset to RMH. Instead of driving the reset signal for 50ms, do so for 3ms	94	But continue to drive 50ms reset signal in warm reset path. Possible to have 2 RMH reset at parallel
Fine Grain Polling on Ports	23	First a delay of 10ms, then followed by fine grain polling at 90us. Normally seeing reset complete within 10-11ms. Still make sure the fine grain polling cover another 10ms range for specification compliance. This time includes Finer grain polling on port reset clear (1.5mS), and Finer grain polling on port enable (3.8mS)
Skip EHCI Controller Reset	20	Intel RC reset EHCI controller in DXE
Skip SetAddress recovery interval for RMH	20	Intel integrated RMH does not need this
Savings for 2 devices	**475.8**	

- Performance varies per number and type of USB devices
- Based on Intel customer reference platform Intel® Core i5 processor with Intel® Series 6 chipset
- Above applies for EHCI, XHCI will be optimized as the technology and products mature.

Agenda

- Responsiveness Introduction
- 2012 Technology Improvements in UEFI
- **Building in Responsiveness**
  - **Motherboard**
  - **Hardware Components**
  - **OS**
  - **UEFI / BIOS**
  - **Developers**
- Summary

Factors Effecting Boot Speed

- **Hardware Power Planes and Power Sequencing**
  - **Provide Separate Power Plane for ME**
  - **Specify tighter than 100mS PCI Spec delay for Power Supplies**
  - **Shorten Power Button De-bounce in Embedded Controllers**
  - **Specify Display Panel timing to what the HW is capable of, not specification**
- **Storage Solution Selection**
  - **SSD > 2x faster than HDD**
  - **SSD Data Readiness timing**
  - **SATA2 vs. SATA3**
- **SPI**
  - **Higher Frequency is better**
  - **Number of Bytes per Read**

Build the motherboards for speed

Talk with your Suppliers

Select the right parts

Factors Effecting Boot Speed

- **Processor**
  - Higher Frequency is better
  - Less No. of Cores/Threads is faster boot, but slower runtime performance
- **Main Memory**
  - Higher Frequency is better
  - Less No of Banks is faster boot, but slower runtime performance
- **Video & Graphics**
  - Controller & Panel Timings important
  - UEFI Graphic Output Protocol driver is faster
  - Single Graphics solution is faster
- **Security**
  - Trusted Platform Module will add time
  - Secure & Measured Boots will add time
- **Platform Features**
  - More Complex the solution, the longer it may take to boot (RAID example)
  - Remote Boot enabled and checked will affect boot

Work with your IHVs

Be aware of trade offs

Factors Effecting Boot Speed

- OS Needs/Requirements
  - Reduce OS Image Size
  - Enable User Interface sooner
  - Needing Keyboard as a boot device
- Enable Class 3 UEFI Solution
  - No CSM support
- Tool used to measure speed
  - Injects delays if not done properly
  - Methods may vary per tool used
- Security
  - Trusted Platform Module will add time
  - Secure & Measured Boots will add time
- Platform Features
  - More Complex the solution, the longer it may take to boot (RAID example)
  - Remote Boot enabled and checked will affect boot

Work with your IHVs

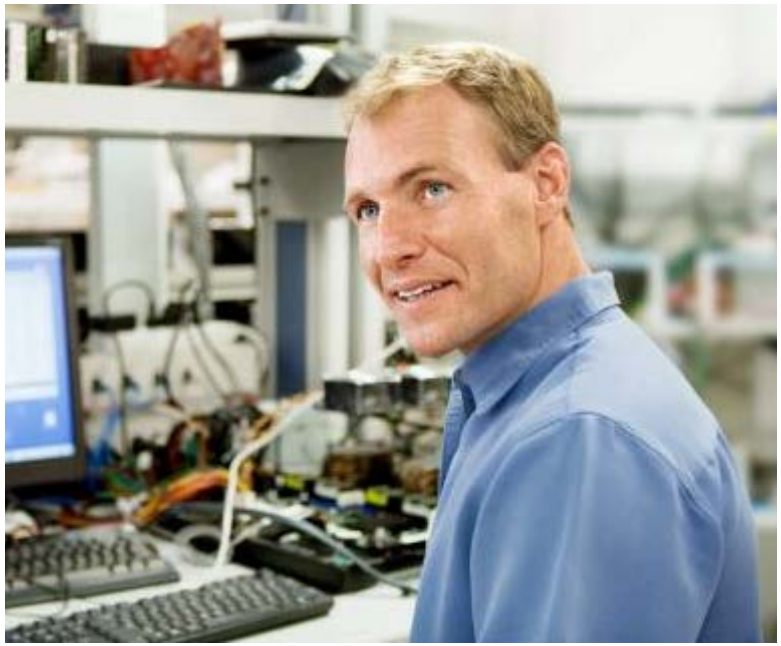
Be aware of trade offs

Factors Effecting Boot Speed

- **A Pessimistic Mentality in System Developers**
  - **"It's only a few Milliseconds"**
  - **"S3 is fast enough"**
  - **"It's a systemic problem"**
  - **"Even if the BIOS disappears, the OS is still slow"**

Don't Ignore YOUR role in Responsiveness

Agenda



- Responsiveness Introduction
- 2012 Technology Improvements in UEFI
- Building in Responsiveness
- **Summary**

Intel 2012 Responsiveness Technologies: Improves User Experience

Off

Intel® Rapid Start Technology

Instant On to active PC applications

Active

Intel® Smart Response Technology

Snappy performance

PC Saves Power

Idle / Suspend

Intel® Smart Connect Technology

Active Resume BIOS Update

Intel® Rapid Start Technology

PC Conserves energy by entering low and lower power system states

PC content remains 'fresh' and receives cloud notifications

PC resumes to active state Quickly

UEFI Intelligent Infrastructure makes these technologies happen

IDF2011
INTEL DEVELOPER FORUM

Summary

- Rethink your PC-AT based assumptions about Responsiveness
- Build in Complementary Responsiveness Technologies
  - Active BIOS Resume Update
  - Intel® Rapid Start technology
  - Intel® Smart Response Technology
  - Intel® Smart Connect Technology
- Drive Responsiveness from your HW & UEFI Layers up
- Achieve a more responsiveness with UEFI

Start Today !

Q&A

Tunnel Mountain Intel DQTM57 UEFI 2.3.1 platform

Intel® UDK 2010 Compatible, supports UEFI 2.3.1

Pre-assembled systems available at HDNW, visit

http://www.Tunnelmountain.net

tomk@hdnw.com, (425) 943-5515 ext 42234. Use product name "Tunnel Mountain" when ordering

Comes with class 2 CSM and UEFI enabled firmware
Download site has Class 3 UEFI only firmware(nocsm)

Comes with serial port for debug
Can be ordered with optional ITP connector and socketed SPI flash - AC-SPEC4480

Visit **http://developer.intel.com/technology/efi/uefi-ihv.htm** for the latest information and other IHVs collateral

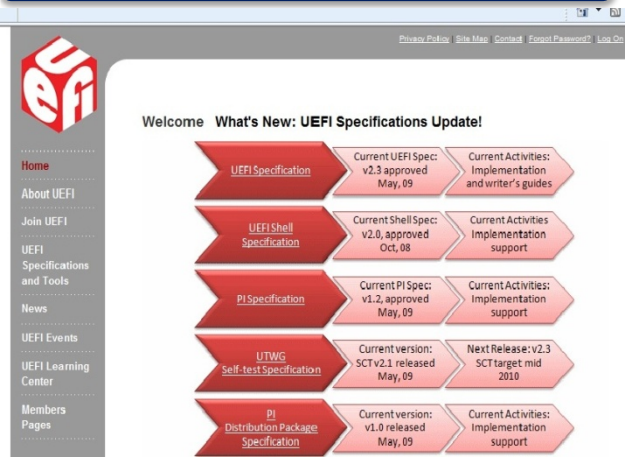
Fall 2011 UEFI Plugfest – Taipei, Oct 24-27

Visit www.UEFI.org for Event Info & Registration

IDF2011
INTEL DEVELOPER FORUM

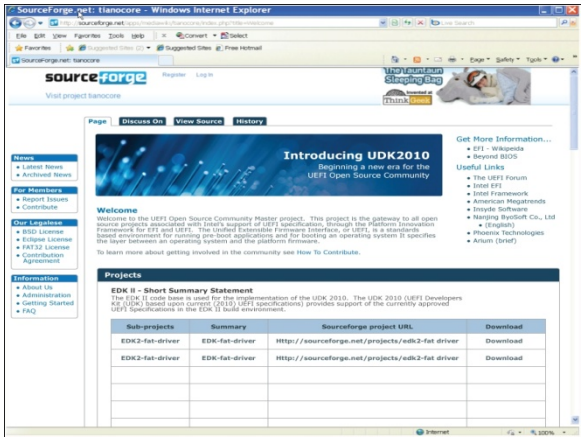
UEFI Industry Resources

UEFI Forum



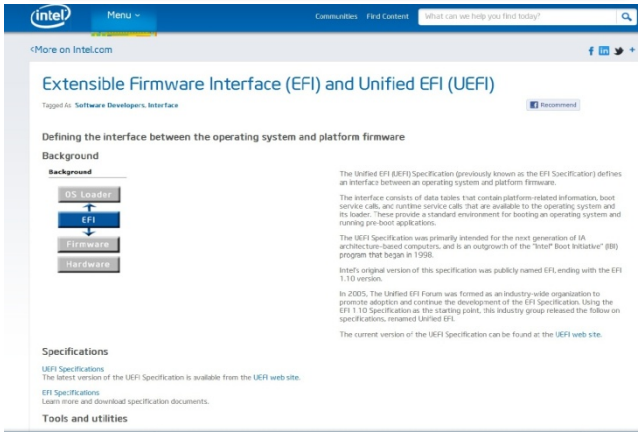
www.uefi.org

UEFI Open Source



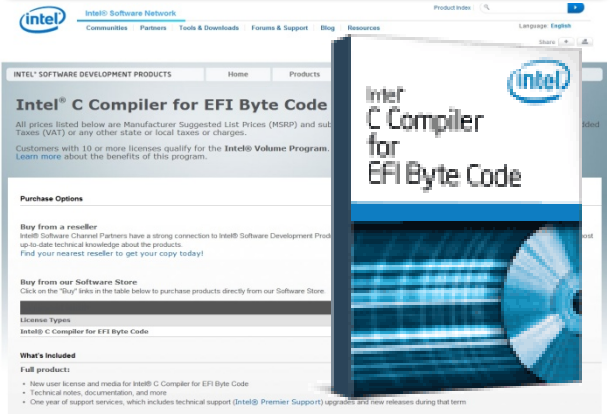
www.tianocore.org

Intel UEFI Resources



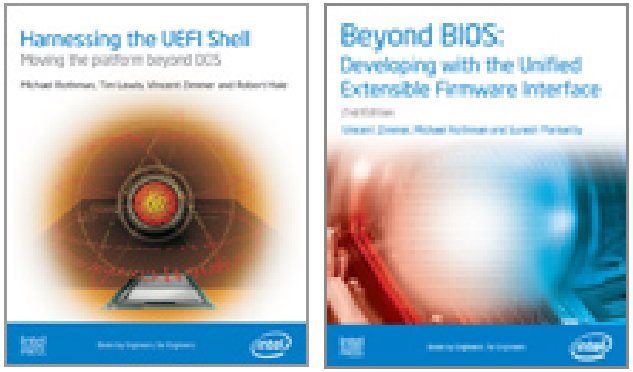
www.intel.com/technology/efi/index.htm

Intel EBC Compiler



http://software.intel.com/en-us/articles/intel-c-compiler-for-efi-byte-code-purchase/

UEFI Books



www.intel.com/intelpress

Training/IHVs Contact

Laurie Jarlstrom
- Intel UEFI Training
- Laurie.Jarlstrom@intel.com

Brian Richardson
- Intel IHVs UEFI Support
- Brian.Richardson@intel.com

IDF2011
INTEL DEVELOPER FORUM

UEFI Sessions Moscone SF IDF 2011

Session ID	Title	Company	Day / Time	Rm
✓ EFIS001	UEFI Security and Networking Advancements	Intel & Insyde SW	Tue 1:05 – 1:55	2009
✓ EFIS002	UEFI Innovations for Platform Security	Intel & AMI	Tue 2:10 - 3:00	2009
✓ EFIS003	Beyond DOS: UEFI Modern Pre-boot Application Development Environment	Intel & Phoenix Tech. LTD	Tue 3:20 - 4:10	2009
✓ EFIS004	Designing for Next Generation Best-In-Class Platform Responsiveness	Intel	Tue 4:25 - 5:15	2009
EFIQ001	Hot Topic Q&A: UEFI in the Industry	All Speakers	Tue 5:25 - 6:00	2009
EFIS005	Microsoft* Windows* Platform Evolution and UEFI Requirements	Intel & Microsoft	Thu 1:05 - 1:55	2005
SPCQ003	Hot Topic Q&A: Intel & Microsoft - Windows * 8	Intel & Microsoft	Thu 2:05 - 2:55	2005

✓ = DONE

IDF2011
INTEL DEVELOPER FORUM

Please Fill out the Online Session Evaluation Form

Be entered to win fabulous prizes everyday!

Winners will be announced at 6pm (Day 1/2) and 3:30pm (Day 3)

You will receive an email prior to the end of this session.

Legal Disclaimer

- INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.
- Intel may make changes to specifications and product descriptions at any time, without notice.
- All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.
- Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.
- Other code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user
- Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.
- Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. Go to: http://www.intel.com/products/processor_number
- Intel product plans in this presentation do not constitute Intel plan of record product roadmaps. Please contact your Intel representative to obtain Intel's current plan of record product roadmaps.
- Intel, Intel® Rapid Start Technology, Intel® Smart Response Technology, Intel® Smart Connect Technology, Intel® 6 & 7 Series Chipset and the Intel logo are trademarks of Intel Corporation in the United States and other countries.
- *Other names and brands may be claimed as the property of others.
-

Risk Factors

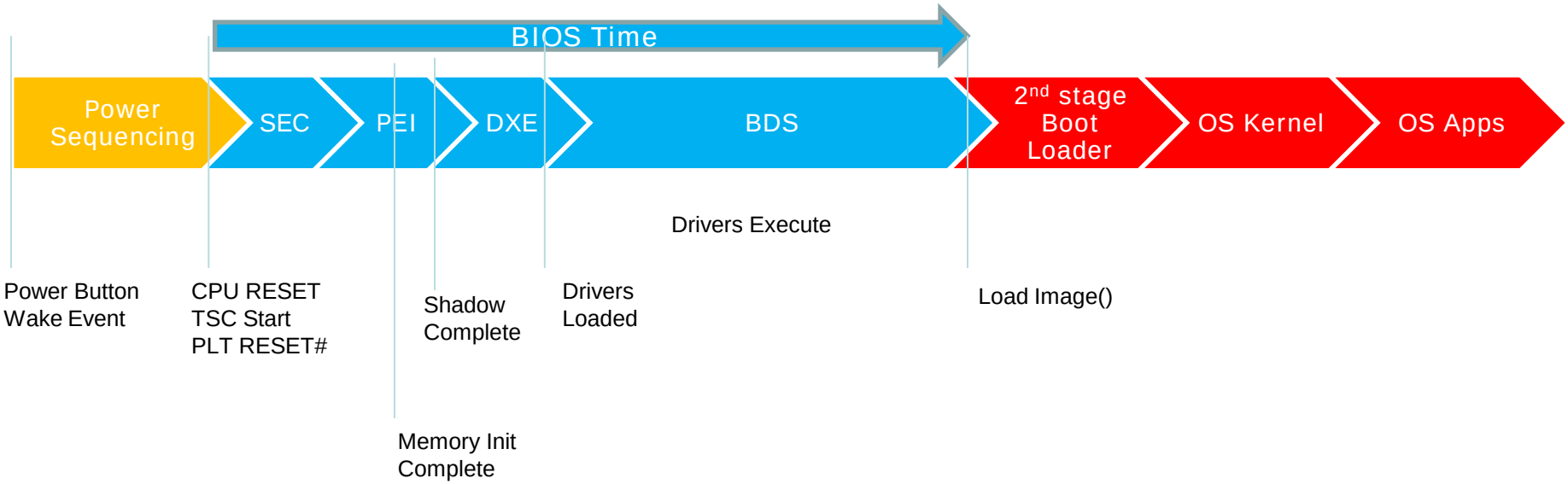
The above statements and any others in this document that refer to plans and expectations for the second quarter, the year and the future are forward-looking statements that involve a number of risks and uncertainties. Words such as “anticipates,” “expects,” “intends,” “plans,” “believes,” “seeks,” “estimates,” “may,” “will,” “should,” and their variations identify forward-looking statements. Statements that refer to or are based on projections, uncertain events or assumptions also identify forward-looking statements. Many factors could affect Intel’s actual results, and variances from Intel’s current expectations regarding such factors could cause actual results to differ materially from those expressed in these forward-looking statements. Intel presently considers the following to be the important factors that could cause actual results to differ materially from the company’s expectations. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions, including supply constraints and other disruptions affecting customers; customer acceptance of Intel’s and competitors’ products; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Potential disruptions in the high technology supply chain resulting from the recent disaster in Japan could cause customer demand to be different from Intel’s expectations. Intel operates in intensely competitive industries that are characterized by a high percentage of costs that are fixed or difficult to reduce in the short term and product demand that is highly variable and difficult to forecast. Revenue and the gross margin percentage are affected by the timing of Intel product introductions and the demand for and market acceptance of Intel's products; actions taken by Intel's competitors, including product offerings and introductions, marketing programs and pricing pressures and Intel’s response to such actions; and Intel’s ability to respond quickly to technological developments and to incorporate new features into its products. The gross margin percentage could vary significantly from expectations based on capacity utilization; variations in inventory valuation, including variations related to the timing of qualifying products for sale; changes in revenue levels; product mix and pricing; the timing and execution of the manufacturing ramp and associated costs; start-up costs; excess or obsolete inventory; changes in unit costs; defects or disruptions in the supply of materials or resources; product manufacturing quality/yields; and impairments of long-lived assets, including manufacturing, assembly/test and intangible assets. Expenses, particularly certain marketing and compensation expenses, as well as restructuring and asset impairment charges, vary depending on the level of demand for Intel's products and the level of revenue and profits. The majority of Intel’s non-marketable equity investment portfolio balance is concentrated in companies in the flash memory market segment, and declines in this market segment or changes in management’s plans with respect to Intel’s investments in this market segment could result in significant impairment charges, impacting restructuring charges as well as gains/losses on equity investments and interest and other. Intel's results could be affected by adverse economic, social, political and physical/infrastructure conditions in countries where Intel, its customers or its suppliers operate, including military conflict and other security risks, natural disasters, infrastructure disruptions, health concerns and fluctuations in currency exchange rates. Intel’s results could be affected by the timing of closing of acquisitions and divestitures. Intel's results could be affected by adverse effects associated with product defects and errata (deviations from published specifications), and by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust and other issues, such as the litigation and regulatory matters described in Intel's SEC reports. An unfavorable ruling could include monetary damages or an injunction prohibiting us from manufacturing or selling one or more products, precluding particular business practices, impacting Intel’s ability to design its products, or requiring other remedies such as compulsory licensing of intellectual property. A detailed discussion of these and other factors that could affect Intel’s results is included in Intel’s SEC filings, including the report on Form 10-Q for the quarter ended April 2, 2011.

Rev. 5/9/11

Agenda

Backup

Typical Power on Flow Button to Browse

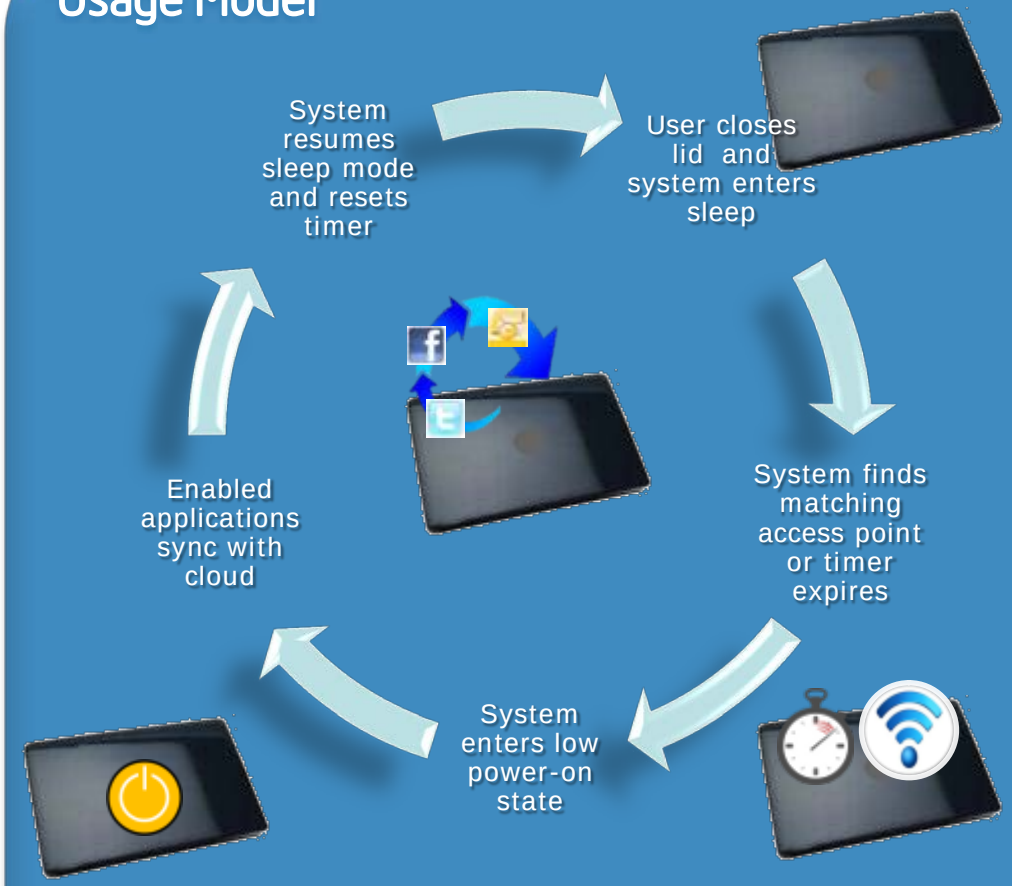


Agenda

- Responsiveness Introduction
- **2012 Technology Improvements in UEFI**
  - Active Resume BIOS Update
  - Intel® Rapid Start Technology
  - Intel® Smart Response Technology
  - **Intel® Smart Connect Technology**
  - Fast USB Enumeration
- Building in Responsiveness
- Summary

Intel® Smart Connect Technology

Usage Model



Benefits

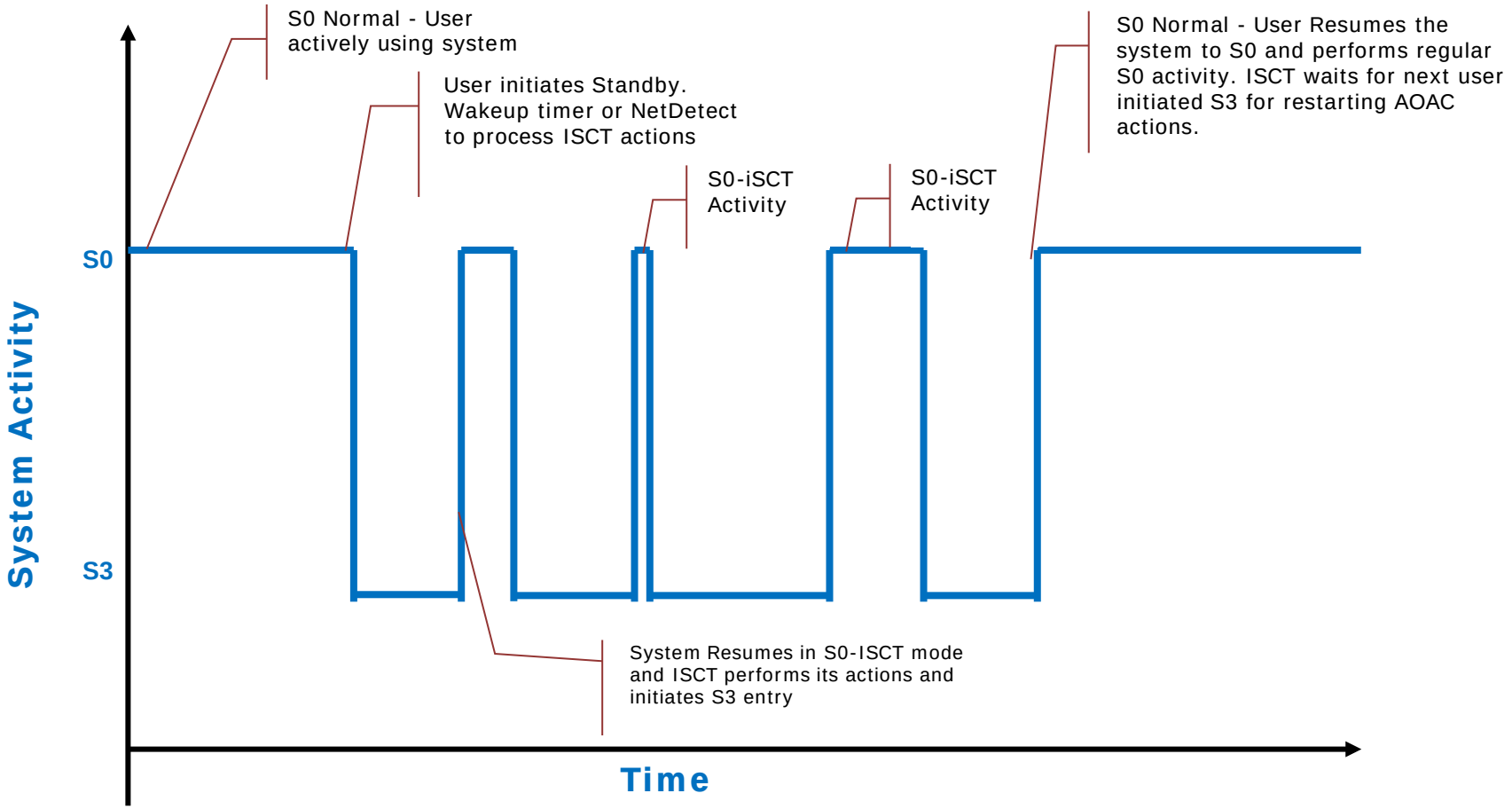
- Desired content is already updated on the system when user wants it
- Content on the system synchronizes with the cloud service, no manual interaction
- Quicker access to internet, data and applications

Intel® Smart Connect Technology
BIOS Requirements

- New Intel Smart Connect Technology ACPI pseudo device object:
  - Toggle Feature On/Off
  - Toggle Notification (LED alerts, etc)
  - Indication of active periodic wakes
  - Toggle Power to WLAN (or WWAN) Module in Sleep, Hibernate, or Intel® Rapid Start Technology
  - Set RTC upon entrance to S3
  - Enables proper Platform Wake Events (EC, Power Button, RTC)
- Enable system to wake via WLAN
- Disable RTC wakes from S4 (OS Hibernate)
  - RTC wakes only to be cleared when BIOS is requested by OS to enter S4

Intel® Smart Connect Technology

State Change Example



Intel® Smart Connect Technology is a new Usage Model

- A new Usage model that improves runtime experience with fresh data on resume

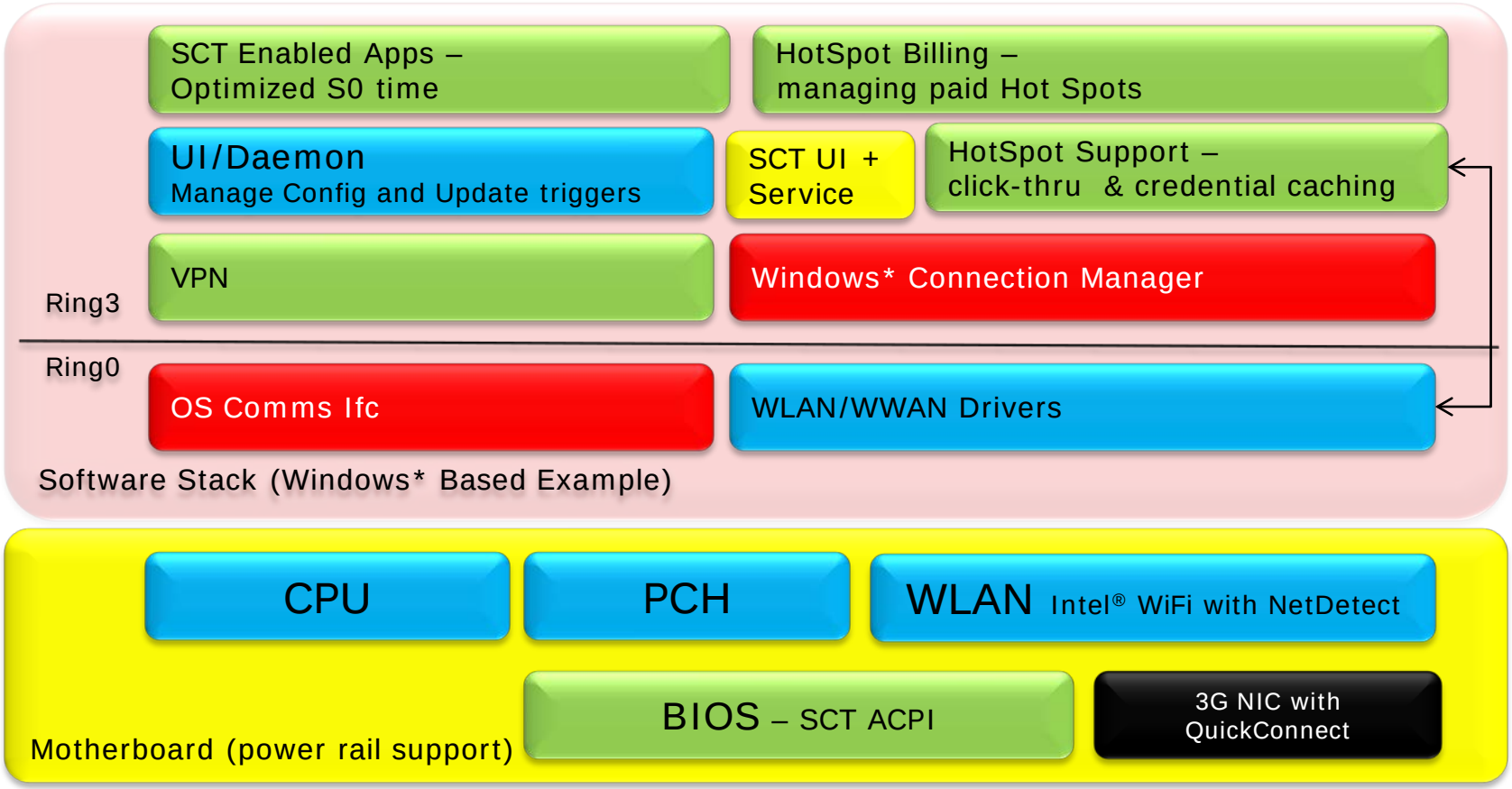
- Performance/Feature benefits enhanced with:
  - SSD installed vs. an HDD
  - Intel® Smart Response Technology
  - Intel® Rapid Start Technology
  - Active Resume BIOS Update
  - Better OS & Application resume and suspend time

- Ask your BIOS vendor and Software Vendor about support

Contact your Intel Field Sales representative for more information

Platform Architecture Overview

Intel® Smart Connect Technology (SCT)



Complete solution stack delivering seamless connectivity experience

Supplier Key: Intel | OS | OEM/SP | IHV | ISV/IBV

Intel Smart Connect Technology ACPI Extensions

Control Method	Description
GABS	Get Intel Smart Connect Technology BIOS Enabled Setting
GAOS / SAOS	Get/Set Intel Smart Connect Technology Function Status
GANS / SANS	Get/Set Intel Smart Connect Technology Notification Status
GWLS / SWLS	Get/Set WLAN Module Status
GWWS / SWWS	Get/Set WWAN Module Status
SASD	Set Intel Smart Connect Sleep Duration
GPWR	Get Platform Wake Reason

Agenda

UEFI BIOS Start &
Finish Line

Time Measurement at “Finish Line”

- Starting line is CPU RESET exit
- Finish Line is “start of call to LoadImage() on the successful boot target”
  - Same for built-in EFI shell or EFI Boot Manager (x64 Windows)
    - Keep logging all LoadImage() for multiple boot targets
    - Report the LoadImage() call of the 1st successful boot target image as BDS end-point
  - INT19 is equivalent to “connect to device with the image to load”
    - Close to LoadImage() of the successful OS load
- TSL (Transient System Load) phase overlaps with OS Loader
  - TSL phase is described in the Framework as the time before the final OS environment
  - TSL phase starts when BDS phase ends
  - TSL phase ends when ExitBootServices() is called (regardless if INT19 legacy interface is used or not)
- DP64.efi will show BIOS boot time as SEC+PEI+DXE+BDS
  - TSL time will be shown but not counted towards BIOS Boot Time
  - TSL time + BIOS Boot time will give us closer number compared to Xperf (Windows) tool view of BIOS POST time.