IDF2012
INTEL DEVELOPER FORUM

Advanced UEFI Development Environment for Embedded Platforms

Jin Lei, Technical Marketing Engineer, Intel
Zhou Pengcheng, Development Manager, Byosoft*
Jiang Bo, Chief Technology Officer, SBS*

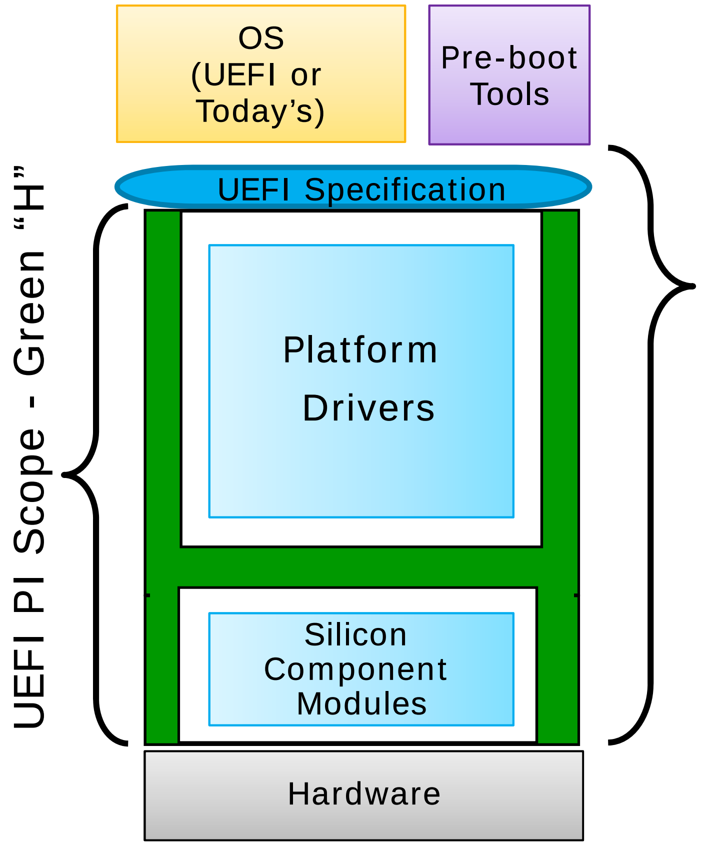
PTAS003

Sponsors of Tomorrow. intel

Agenda

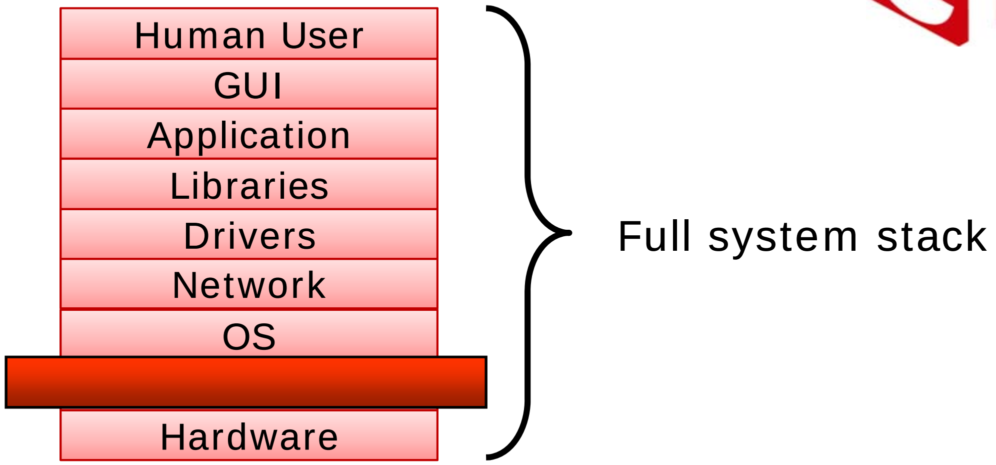
- UEFI Development Environment for Embedded Platforms
- Byosoft* Embedded Development Best Known Method
- SBS* Embedded Application Experience Sharing
- Summary

UEFI Technology Overview



🟩 PEI/DXE PI Foundation

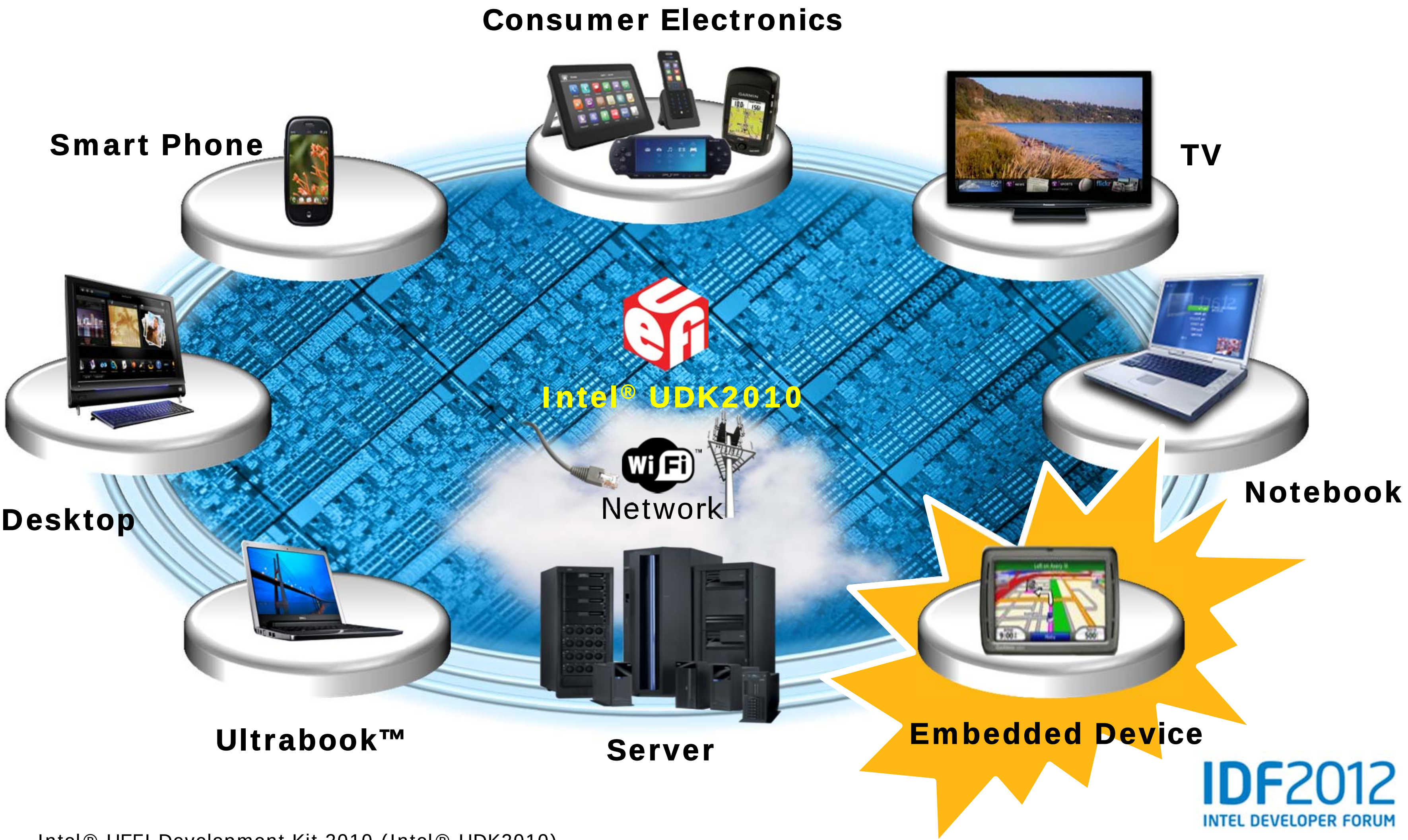
🟦 Modular components



- Unified Extensible Firmware Interface (UEFI) specifies how firmware boots OS loader
- UEFI's Platform Initialization Architecture (PI) specifies how UEFI firmware initializes Si and the platform
- UEFI and PI specifications are governed by UEFI forum (www.uefi.org)
- Intel® UDK2010 is a reference implementation of UEFI and PI specifications

Visit www.intel.com/udk for details

Intel® UDK2010 Standard Foundation for the Compute Continuum



Firmware Difference Between PC and Embedded Market

Metric	PC	Embedded
OS Support	Full range	Embedded Linux*, Android* & Windows* Embedded
Distribution Model	Thru IBV	Direct to Customer
Boot Speed	PC Optimized (~>2 seconds)	Optimized for CE and Handheld (~< 1 second)
Footprint	PC Optimized (~>1 MB)	Optimized for CE and Handheld (~< 256 KB)

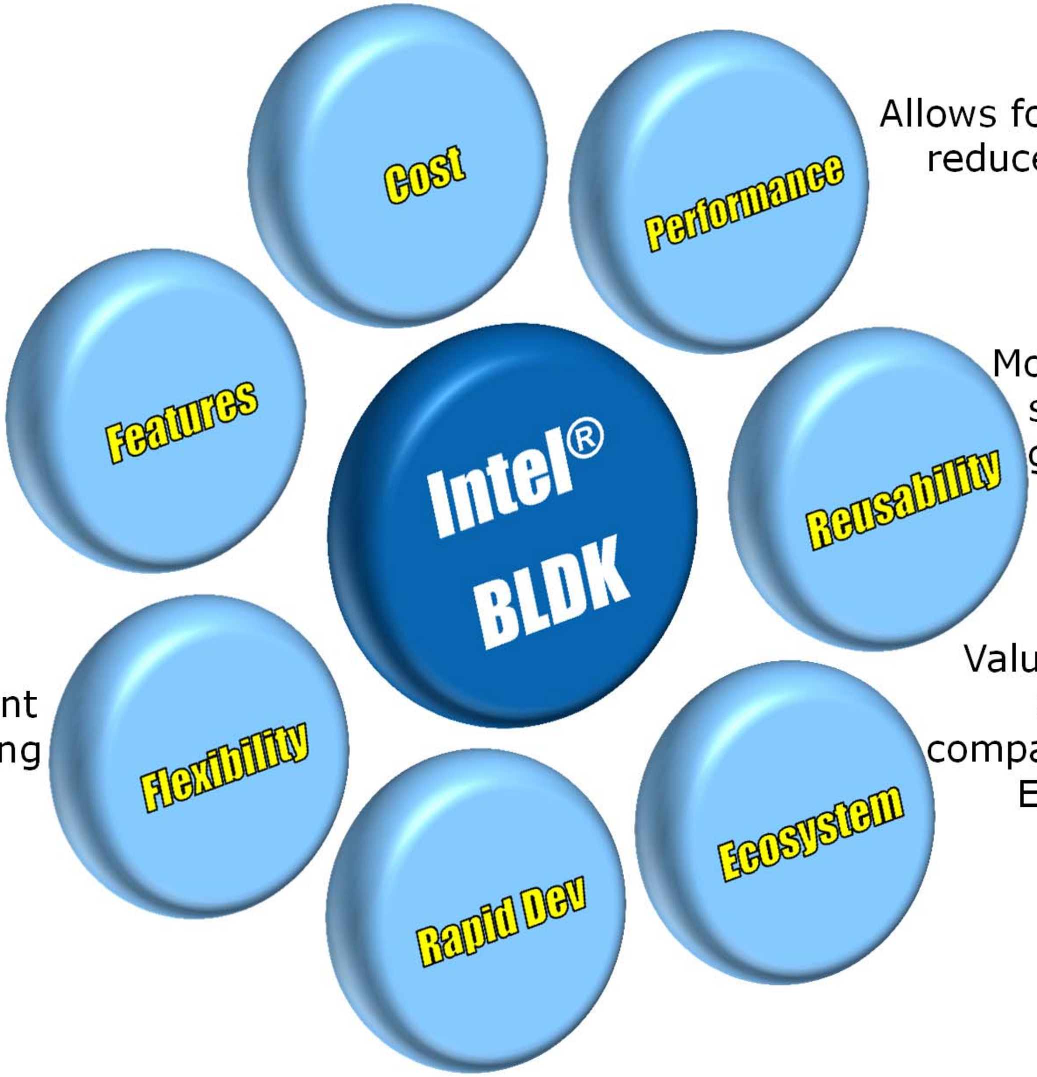
The Needs of Embedded Systems Developers are very different from PC

Meeting the Needs of Embedded Systems Developers

Features:
Rich set of boot time features and capabilities

Flexibility: Provides flexibility and control for customization

Rapid Development:
Tools speed development by abstracting underlying code



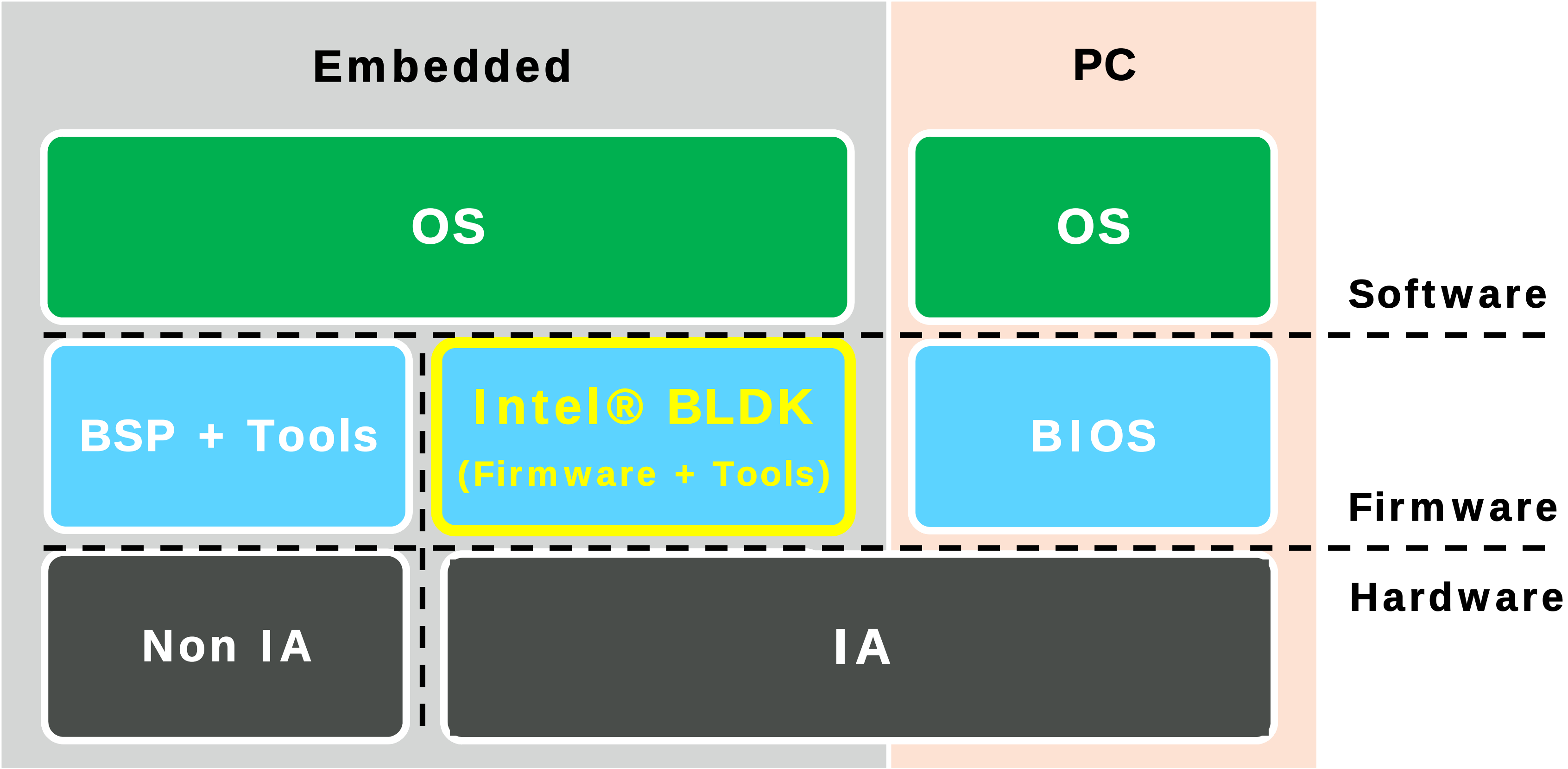
Performance:
Allows for optimization for reduced boot times and firmware size

Reusability:
Modularity and UEFI standards ensures greater reusability across platforms

Ecosystem:
Value-added products and services from companies in the Intel® Embedded Alliance

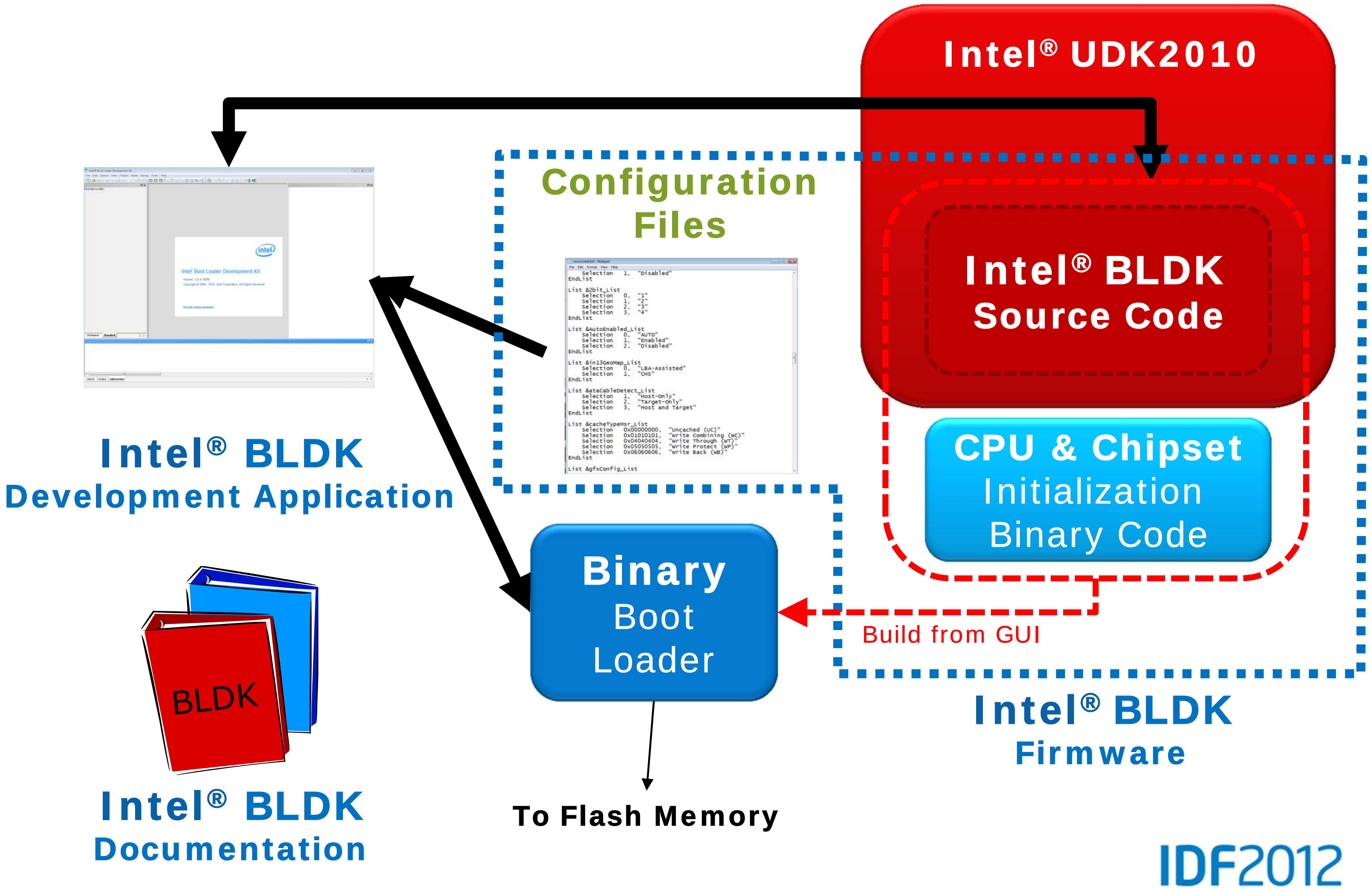
IDF2012
INTEL DEVELOPER FORUM

Stack Difference Between PC and Embedded



Intel® BLDK fills the firmware gap for Intel Architecture (IA) for embedded

Intel® BLDK Major Components



Intel® UDK2010

Configuration Files

Intel® Boot Loader Development Kit

Version: 2.0.0.18289

Copyright © 2009 - 2010, Intel Corporation. All Rights Reserved.

```
    Selection   1,  "Disabled"
EndList

List &2bit_List
    Selection   0,  "1"
    Selection   1,  "2"
    Selection   2,  "3"
    Selection   3,  "4"
EndList

List &AutoEnabled_List
    Selection   0,  "AUTO"
    Selection   1,  "Enabled"
    Selection   2,  "Disabled"
EndList

List &in13GeoMap_List
    Selection   0,  "LBA-Assisted"
    Selection   1,  "CHS"
EndList

List &ataCableDetect_List
    Selection   1,  "Host-Only"
    Selection   2,  "Target-Only"
    Selection   3,  "Host and Target"
EndList

List &cacheTypeMsr_List
    Selection   0x00000000,  "Uncached (UC)"
    Selection   0x01010101,  "Write Combining (WC)"
    Selection   0x04040404,  "Write Through (WT)"
    Selection   0x05050505,  "Write Protect (WP)"
    Selection   0x06060606,  "Write Back (WB)"
EndList

List &gfxConfig_List
```

Intel® BLDK Source Code

CPU & Chipset Initialization Binary Code

Intel® BLDK Development Application

Binary Boot Loader

Build from GUI

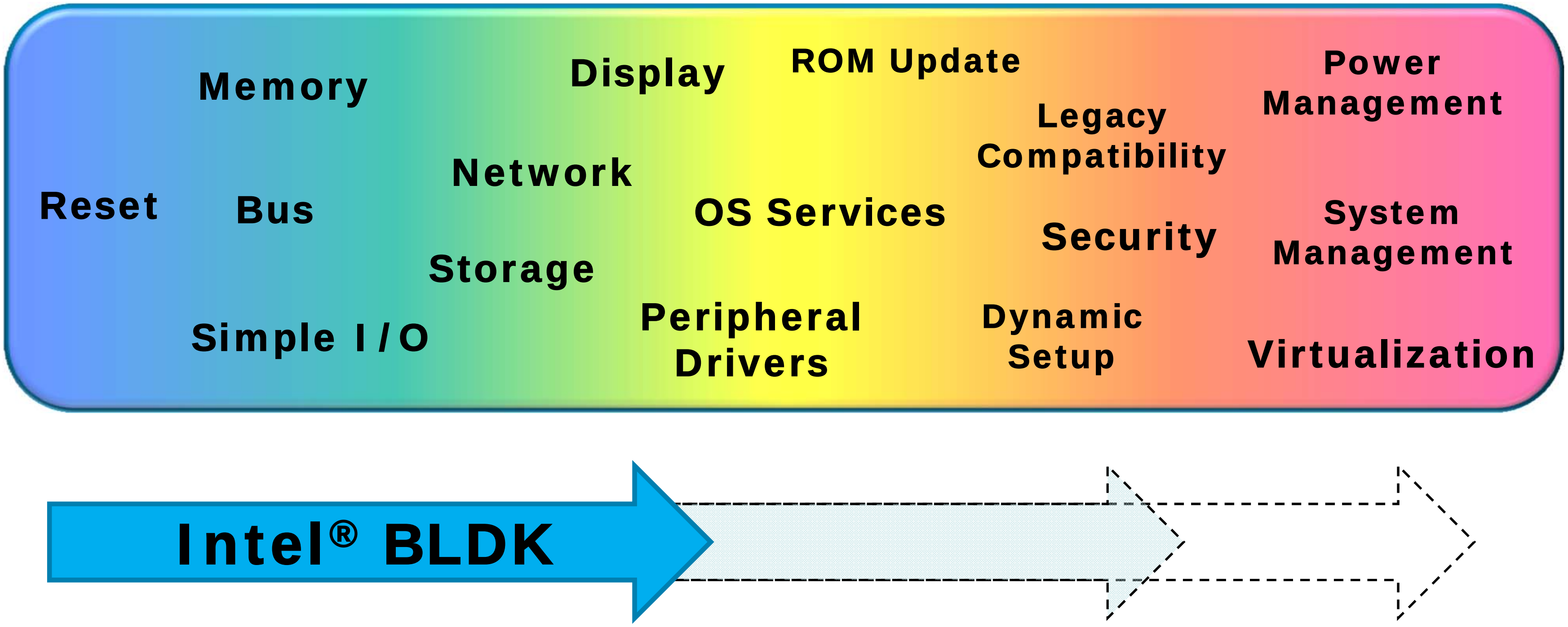
Intel® BLDK Firmware

To Flash Memory

Intel® BLDK Documentation

Intel® Boot Loader Development Kit (Intel® BLDK) Intel® UEFI Development Kit 2010 (Intel® UDK2010)

Spectrum of System Initialization Firmware



Intel® BLDK Provides Flexibility to Scale System Initialization for Embedded Systems

Intel® Boot Loader Development Kit (Intel® BLDK)

Intel® BLDK Fully Supported within the Embedded Ecosystem

Operating System Vendors

OSV

A more integrated stack with firmware and OS

Independent BIOS Vendors

IBV

Development tools, custom boot loader implementations and engineering services

Independent Software Vendors

ISV

Engineering services for boot loader customization

Embedded Board Manufacturers

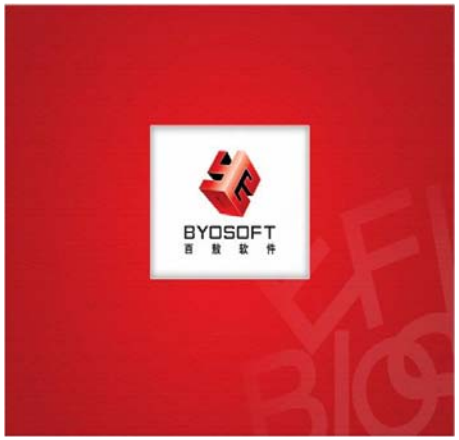
EBM

COTS platforms with customized boot loaders and integrated Board Support Packages, ready for software development

Agenda

- UEFI Development Environment for Embedded Platforms
- Byosoft* Embedded Development Best Known Method
- SBS* Embedded Application Experience Sharing
- Summary

Byosoft* Introduction



- Established in 2006
- Only one local PRC independent BIOS vendor
- Products have been involved Legacy PC, Embedded and Server
- Focus on Chinese Market

Cost Effective

Customer Oriented

Only One PRC IBV

Local PRC Support

Byosoft* BIOS Roadmap

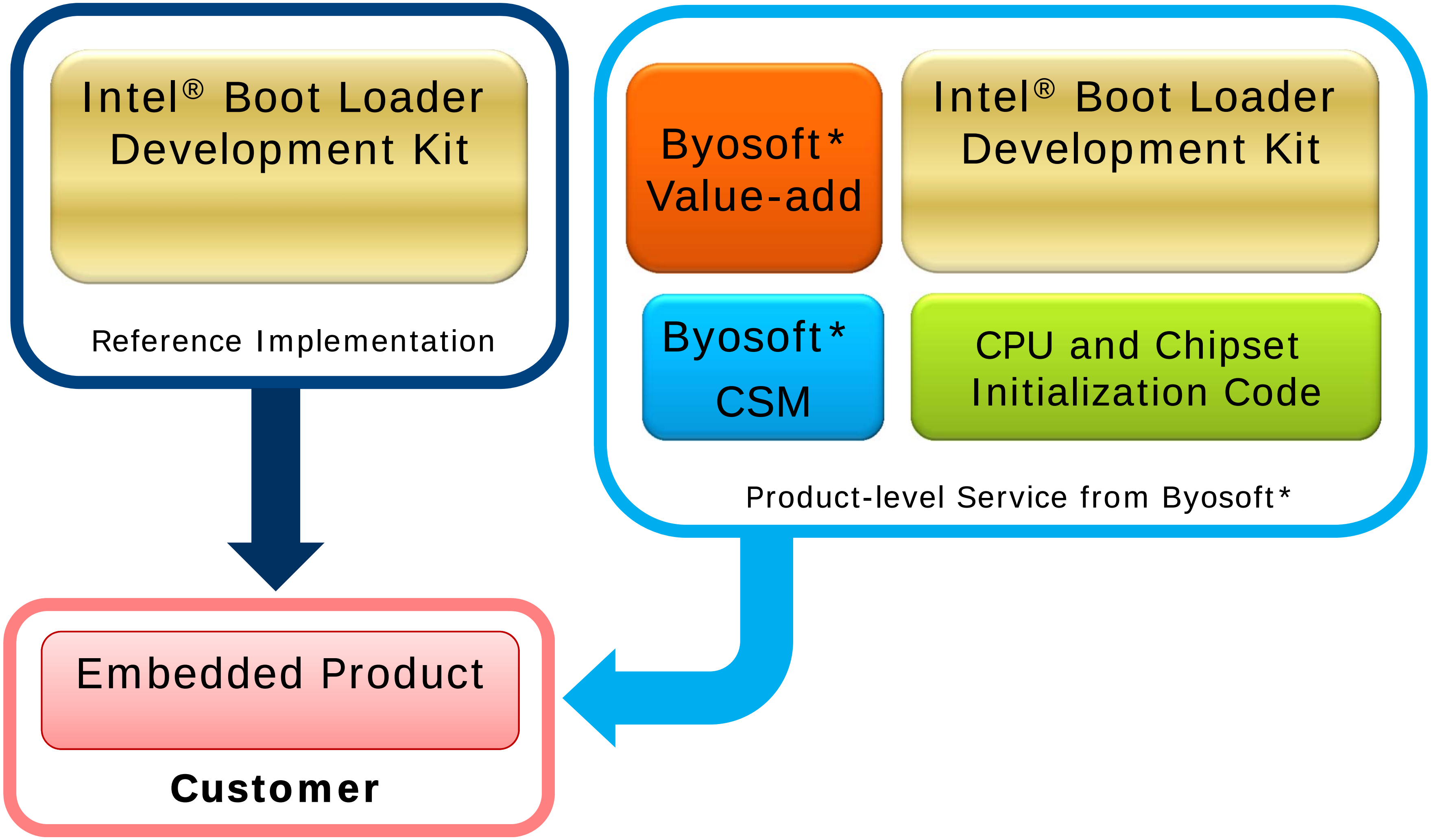
Intel® 处理器	2011	2012	Intel® 平台
Intel® Xeon® 处理器		Romley [Intel Xeon E Series]	服务器平台
Intel® Core™ 处理器	Huron River [Sandy Bridge]	Chief River [Ivy Bridge]	移动平台
	Sugar Bay [Sandy Bridge]	Maho Bay [Ivy Bridge]	台式机平台
Intel® Atom™ 处理器	Crown Bay [Intel Atom E6xx]	Cedar Trail [Intel Atom D/N2000]	嵌入式平台

基于 Intel® UDK2010

基于 Intel® BLDK

Intel® Boot Loader Development Kit (Intel® BLDK)   Intel® UEFI Development Kit 2010 (Intel® UDK2010)

Support Customer with Intel® BLDK



Intel® Boot Loader Development Kit

Reference Implementation

Byosoft* Value-add

Intel® Boot Loader Development Kit

Byosoft* CSM

CPU and Chipset Initialization Code

Product-level Service from Byosoft*

Embedded Product

Customer

*文中涉及的其它名称及商标属于各自所有者资产。

IDF2012
INTEL DEVELOPER FORUM

Byosoft* Comprehensive Boot Loader Features and Support

Features

- Legacy OS Support
- Legacy USB Support
- Security Support
- Compatibility Support
- Remote Network Management
- Graphic UI
- Authentication
- Fast Boot

Support Model based on Intel® BLDK

- Full Source Provider
- Customer Board Porting
- Features Customization
- Technical Consultation and Training

Intel® Boot Loader Development Kit (Intel® BLDK)

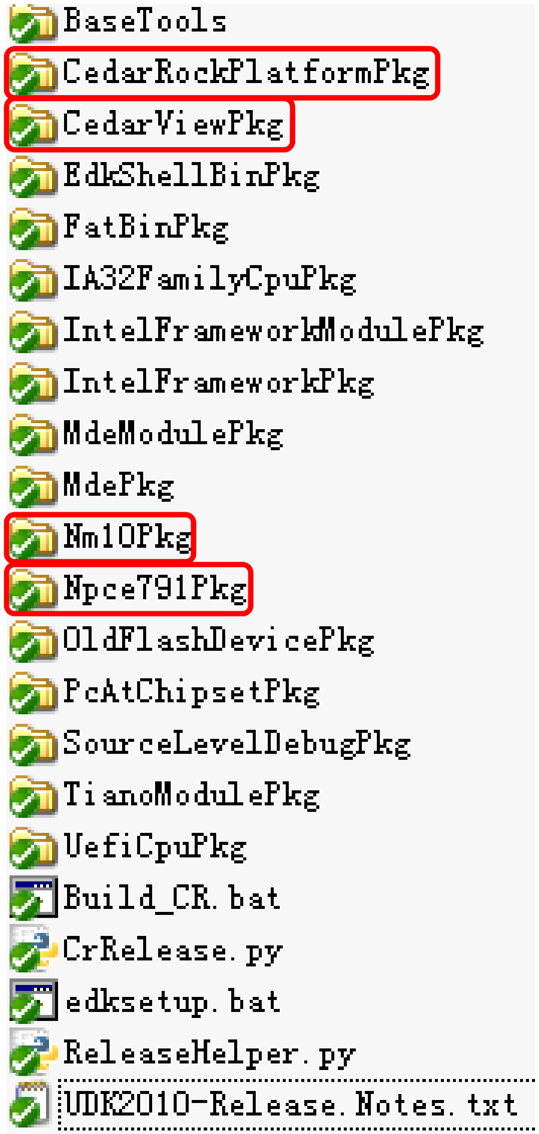
Intel® BLDK Usages BKM

- Platform Porting
- Firmware Customization
- Performance Optimization
- Legacy OS Support
- Network Support

Platform Porting

If you want to port a new platform, you need replace below directory.

- Chipset Directory
  - CedarViewPkg
  - Nm10Pkg
  - Npce791Pkg
- Platform Directory
  - CedarRockPlatformPkg



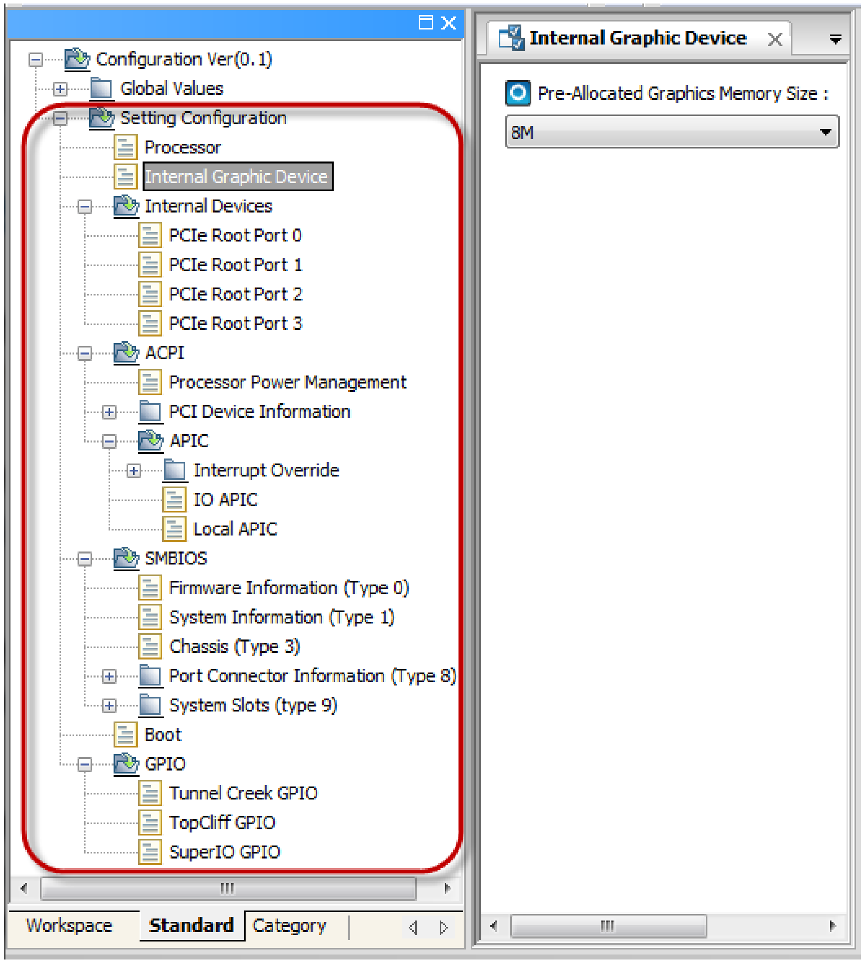
BaseTools
CedarRockPlatformPkg
CedarViewPkg
EdkShellBinPkg
FatBinPkg
IA32FamilyCpuPkg
IntelFrameworkModulePkg
IntelFrameworkPkg
MdeModulePkg
MdePkg
Nm10Pkg
Npce791Pkg
OldFlashDevicePkg
PcAtChipsetPkg
SourceLevelDebugPkg
TianoModulePkg
UefiCpuPkg
Build_CR.bat
CrRelease.py
edksetup.bat
ReleaseHelper.py
UDK2010-Release.Notes.txt

Firmware Customization

- Development Application provides the ability to customize firmware

- Hundreds of firmware options are configurable through the Development Application

- No source modification is required



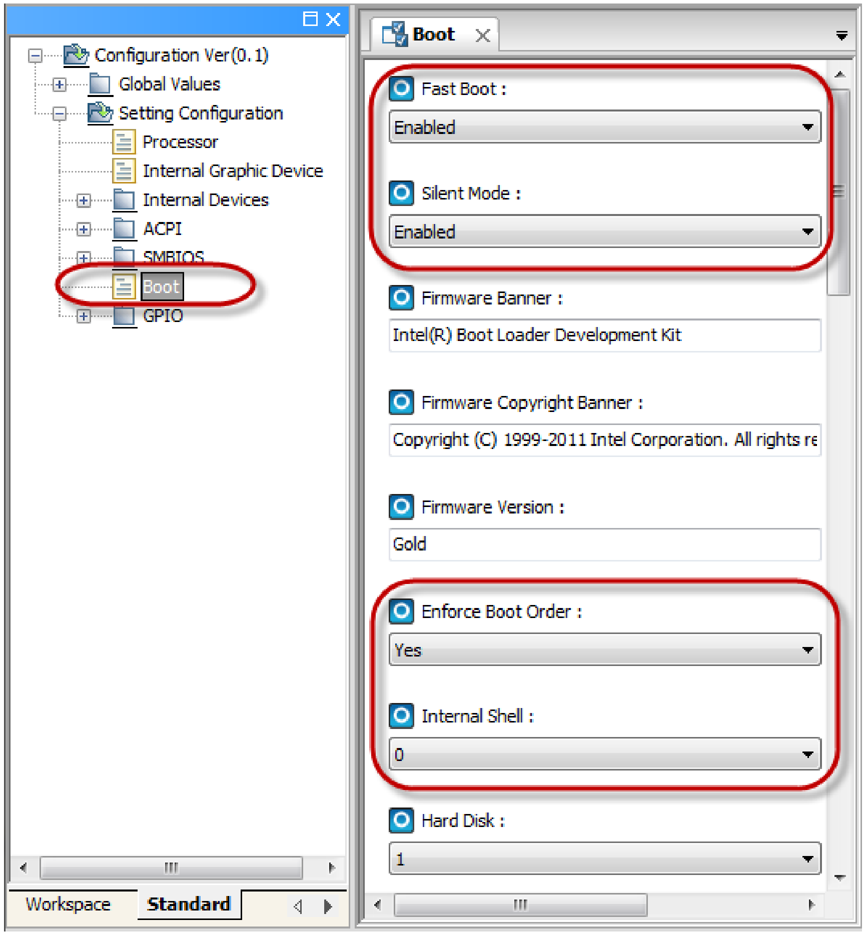
Pre-Allocated Graphics Memory Size : 8M

Performance Optimization

- Intel® BLDK boot sequence can be configured for fast boot via the Development Application

- Only drivers required for system boot are dispatched

- Faster boot times can be achieved by optimizing Intel BLDK for a specific target configuration



Fast Boot : Enabled

Silent Mode : Enabled

Firmware Banner : Intel(R) Boot Loader Development Kit

Firmware Copyright Banner : Copyright (C) 1999-2011 Intel Corporation. All rights re

Firmware Version : Gold

Enforce Boot Order : Yes

Internal Shell : 0

Hard Disk : 1

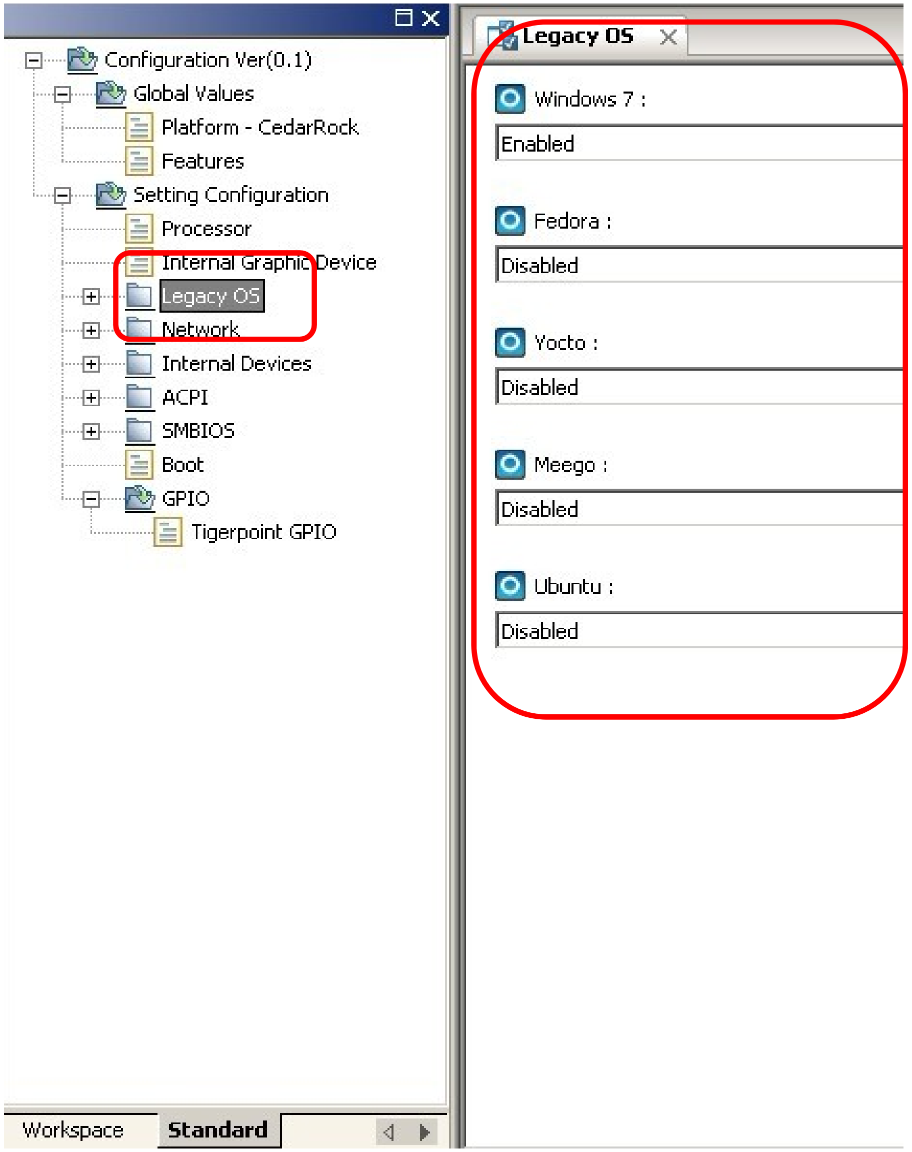
Legacy OS Support

- Embedded System need Multiple OS Support
- CSM is a key module to support Legacy OS

If you want to add CSM support, you need add below driver.

```
#
# Legacy Modules
#

PcAtChipsetPkg/8259InterruptControllerDxe/8259.inf
TianoModulePkg/Csm/LegacyBiosDxe/LegacyBiosDxe.inf
TianoModulePkg/Csm/BiosThunk/VideoDxe/VideoDxe.inf
TianoModulePkg/Csm/BiosThunk/BlockIoDxe/BlockIoDxe.inf
TCPlatformPkg/LegacyBiosPlatformDxe/LegacyBiosPlatformDxe.inf
ByoModulePkg/Csm/LegacyUsb/ LegacyUsb.inf
```



Windows 7 : Enabled

Fedora : Disabled

Yocto : Disabled

Meego : Disabled

Ubuntu : Disabled

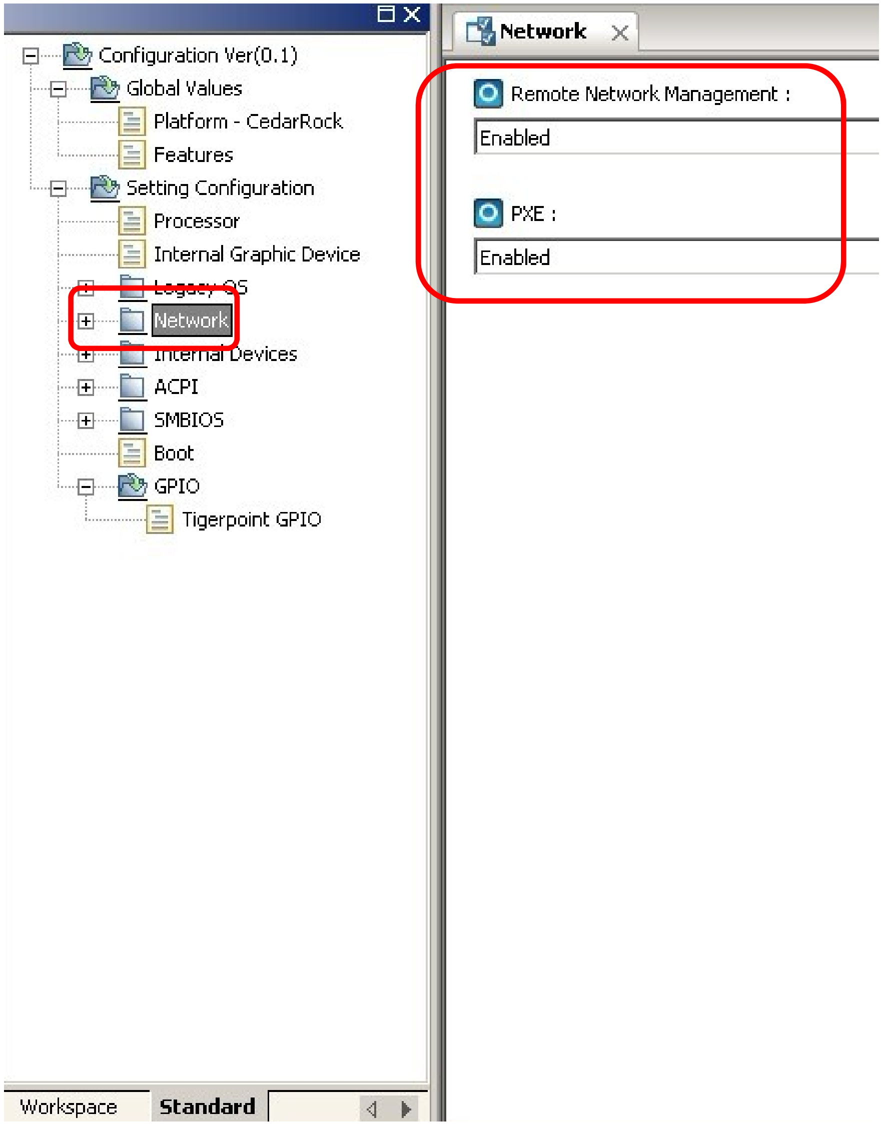
Network Support

- Support Remote Network Management
- Support PXE Function

If you want to add Network support, you need add below driver.

```
#
# Network Modules
#

TianoModulePkg/Network\Ip4ConfigDxe\Ip4ConfigDxe.inf
TianoModulePkg/Network\Ip4Dxe\Ip4Dxe.inf
TianoModulePkg/Network\Tcp4Dxe\Tcp4Dxe.inf
                                        .
                                        .
```



Remote Network Management : Enabled

PXE : Enabled

Agenda

- UEFI Development Environment for Embedded Platforms
- Byosoft* Embedded Development Best Known Method
- SBS* Embedded Application Experience Sharing
- Summary

SBS* Introduction

- Founded in 1992, SBS Science & Technology Co., Ltd.
- The first member of PC/104 Consortium, PICMG Organization and Intel® Embedded Alliance.
- The leading provider of embedded computing solutions in Chinese market.
- Headquartered in Shenzhen, with a number of branch offices in Beijing, Shanghai, Xi’an, Nanjing, Jinan, Shenyang, Chengdu, Wuhan, Guangzhou, etc.

SBS* Embedded Market Focus

Healthcare Devices

Retail Kiosks

Digital Signage

IVI System

Electric Power System

Train Monitoring System

Intelligent Transport System

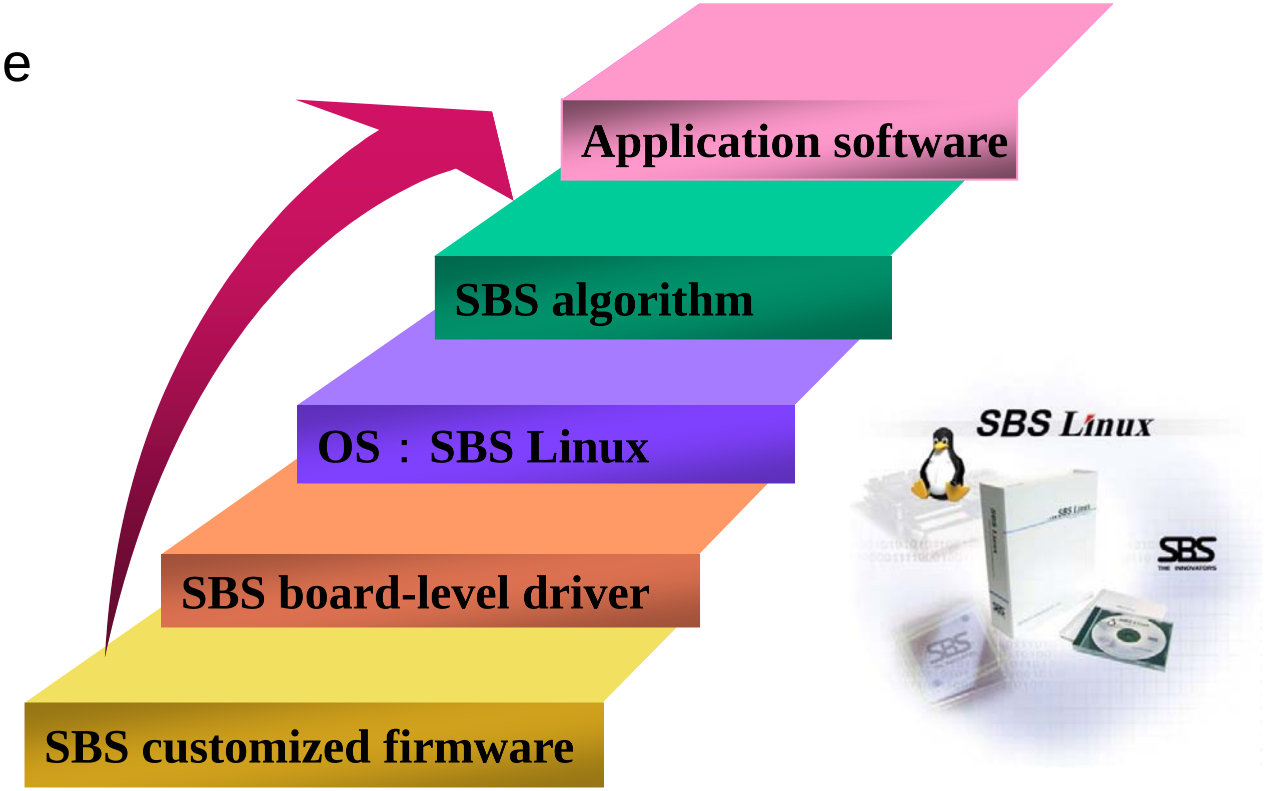
Metro AFC System

Embedded Software Requirements

- Modularity, easy for customization
- Fast boot is key for embedded
- Real-time, quick response
- Comprehensive test
- Product differentiation

SBS* Embedded System

- High Reliability
- Low Power Consumption
- Long Product Life
- Upgradeable
- Small Size



Application software

SBS algorithm

OS：SBS Linux

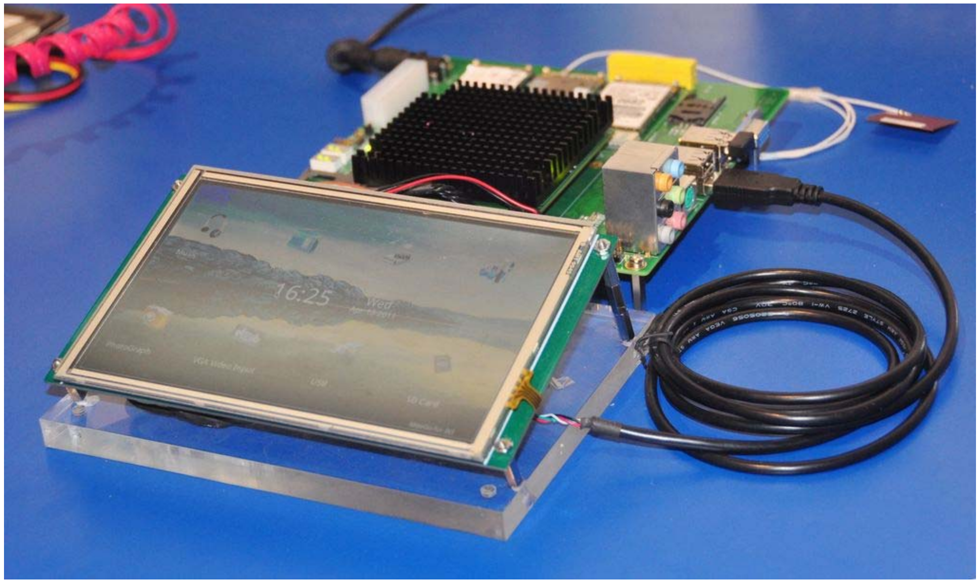
SBS board-level driver

SBS customized firmware

Intel® BLDK Meets SBS* Embedded Requirements

- Get rid of legacy BIOS
- Customized and Professional
- Easy for Differentiation
- Fast Boot
- IP Protection

Application Example Based on Intel® BLDK



- Fast boot
  - Power to OS < 2s (BLDK < 1s)
- Easy to Customize Hardware
- Able to Support Multiple Boot Path

Using Intel® Atom™ E6xx platform and Intel® BLDK, SBS* was able to deliver the competitive In-vehicle infotainment (IVI) product

SBS* Product Samples Based on Intel® BLDK

Intel® Atom™ Processor E6xx Series

COMe9440 (55mm X 84mm)

Intel® Atom™ Processor E6xx Series

SCM-9200 (96mmX96mm)

Intel® Atom™ Processor N/D 2000 Series

STM9040 (70mm X 84mm)

Intel® Atom™ Processor N/D 2000 Series

STM9060 (62mm X 68mm)

IDF2012
INTEL DEVELOPER FORUM

Agenda

- UEFI Development Environment for Embedded Platforms
- Byosoft* Embedded Development Best Known Method
- SBS* Embedded Application Experience Sharing
- **Summary**

Summary

- Intel® BLDK is a royalty-free solution for fixed-function embedded devices
- Intel BLDK is a complete solution that includes source, binaries, debug tools and documentation
- Intel BLDK reference implementations available now for:
  - Intel® Atom™ Processor E6xx Series
  - Intel Atom Processor E6x5C Series
  - Coming Soon:
    Intel Atom Processor N2000 and D2000 Series

Fast · Simple · Flexible

Call to Action

- Download Intel® BLDK and related whitepapers and documentation (http://intel.com/go/bldk)
- Experiment with Intel® BLDK on your Intel reference platform
- Identify 3rd parties that can assist with development efforts
(http://intel.com/go/eca)
- Visit the online community support forum
(http://edc.intel.com/community)

Related Sessions

Session ID	Title	Day	Time	Room
✓ PTAC001	Poster Chat: UEFI Application Development using Standard Libraries and Python*	Wed	14:00 16:25	Station 7
✓ PTAC002	Poster Chat: Power and Thermal Analysis using Intel® Platform Profiling Tool	Wed	14:00 16:26	Station 8
✓ PTAS001	System Behavior and Performance Prediction using System Modeling and Simulation Tools	Wed	14:15	310
✓ PTAS002	Shift Left! Leverage Full System Simulation to Reduce Your Time To Market	Wed	15:20	310
✓ PTAS003	Advanced UEFI Development Environment for Embedded Platforms	Wed	16:25	310
PTAQ001	Platform Technologies and Analysis Q&A	Wed	17:15	310
PTAS004	Implementing Platform Security with UEFI	Thurs	13:10	306B
PTAS005	Platform Optimization Using Open Computing Language (OpenCL*) Tool	Thurs	14:15	306B
	Software and Services Group Pavilion - Platform Technologies: UEFI, Analysis Tools, and Simulation Booth Number 16	Wed - Thurs		Show Case

✓ = DONE

Please Fill out the Online Session Evaluation Form

Be entered to win fabulous prizes everyday!

Winners will be announced at 8pm today

You will receive an email prior to the end of this session
Fill out the evaluation by 7pm today to be entered for the prizes

Sweepstakes rules available at Information desk

IDF2012
INTEL DEVELOPER FORUM

Q&A

IDF2012
INTEL DEVELOPER FORUM

Risk Factors

The above statements and any others in this document that refer to plans and expectations for the first 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. Uncertainty in global economic and financial conditions poses a risk that consumers and businesses may defer purchases in response to negative financial events, which could negatively affect product demand and other related matters. 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. Intel is in the process of transitioning to its next generation of products on 22nm process technology, and there could be execution and timing issues associated with these changes, including products defects and errata and lower than anticipated manufacturing yields. 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. 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. 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. 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 Oct. 1, 2011.

Rev. 1/19/12

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.

- A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.
- Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.
- The products described in this document 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.
- 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.
- Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.
- Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm
- Sandy Bridge, ivy Bridge, Crown Bay, Cedar Trail, Romley, Moho Bay, Sugar Bagy, Chief River and 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
- Intel, Sponsors of Tomorrow, Core, Xeon, Atom 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.
-