UEFI Development and Innovations for System-On-Chip (SoC)

Xing Kenly, Senior BIOS Engineer, Intel
Zhou Eric, Senior Engineering Manager, Byosoft

EFIS002

Sponsors of Tomorrow.™ intel

Agenda

- Why use Intel® UEFI Development Kit 2010 (Intel® UDK2010) in System-On-Chip (SoC)
- Enable Intel® Atom™ Processor E6xx with Intel® UDK2010
- Byosoft* SoC Boot Loader Development

Agenda

- Why use Intel® UEFI Development Kit 2010 (Intel® UDK2010) in System-On-Chip (SoC)
- Enable Intel® Atom™ Processor E6xx with Intel® UDK2010
- Byosoft* SoC Boot Loader Development

System-On-Chip (SoC) & SoC Firmware

- What is SoC
  - SoC is a single chip which integrates a complete set of system components
  - Usually contains a processor core, utilizes standard interconnects & busses and requires software components for full operation
- What is SoC firmware?
  - SoC firmware is coded instructions that are stored permanently in read-only memory
  - When the device starts up, the SoC firmware is to initialize and identify system devices. The primary function of the firmware is to load and start an operating system.

IDF2011
INTEL DEVELOPER FORUM

The Requirements of SoC Firmware

Perspective of Product

Stable

Stability is essential for industry control devices

Performance

Like in IVI devices, boot speed is one of the key indicators

Perspective of Development

Low Technical Threshold

Easy to learn, easy to use

Customization

Meet the requirements of time to market for different segment devices

Need a Firmware Solution for SoC

IVI: In-Vehicle Infotainment

SoC: System-on-Chip

IDF2011 INTEL DEVELOPER FORUM

Intel® UDK2010 Enables a Common Firmware Development Foundation Across the Compute Continuum

The Intel® UDK2010 is an open source build environment and tools that supports the development of UEFI Firmware, drivers and applications.

IDF2011 INTEL DEVELOPER FORUM

Intel® UDK2010 is a Good Option for SoC

Perspective of Product

Stable

Like in some industry control devices

The core of Intel UDK2010 has been verified on server, desktop, laptop…

Performance

Like in IVI devices, boot speed is one of the key indicators

Intel UDK2010 has a leading boot performance

Perspective of Development

Low Technical Threshold

Intel UDK2010 is C language and development environments are Windows*/Linux*/Ios*

Customization

Meet the requirements of time to market for different segment devices

Intel UDK2010 naturally supports customization with its special features, like modular packages…

Intel® UDK2010 meets the requirements of SoC firmware

Intel® UDK2010: Intel UEFI Development Kit 2010

SoC: System-on-Chip

IDF2011 INTEL DEVELOPER FORUM

Other Reasons to Choose Intel® UDK2010 for SoC Firmware

- ✓ Compatible with Industry standards, like UEFI spec, PI spec
- ✓ Bundle of complex features, like ACPI
- ✓ Open source community contribution
- ✓ Support by ecosystem, IBVs/ISVs/OSVs/IHVs

Intel® UDK2010 is on http://www.tianocore.sourceforge.net

SoC: System-on-Chip
Intel® UDK2010: Intel® UEFI Development Kit 2010

Agenda

- Why use Intel® UEFI Development Kit 2010 (Intel® UDK2010) in System-On-Chip (SoC)
- **Enable Intel® Atom™ Processor E6xx with Intel® UDK2010**
- Byosoft* SoC Boot Loader Development

Intel® Atom™ Processor E6xx Series Architecture

North complex

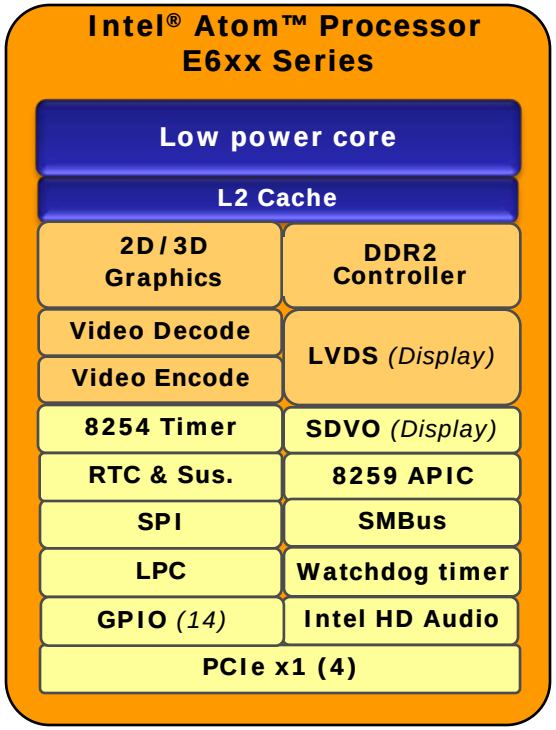
Single Intel® Atom™ Processor Core
- 45nm Hi-K process
- Max 512K L2 cache
- 0.6 to 1.6GHz Low power core

Memory controller
- 32-bit DDR2 667/800
- Max 1GB
- Single Memory Channel

Graphics
- 2D and 3D HW accelerator

Integrated High Definition Video Decoder & Encoder

Display
- LVDS & *SDVO interface*



South complex

LPC
- 8254
- HPET
- Watch Dog
- RTC & CMOS
- 14-pins GPIO
- 8259

SPI Interface

SMBUS1.0

Intel® High Definition Audio

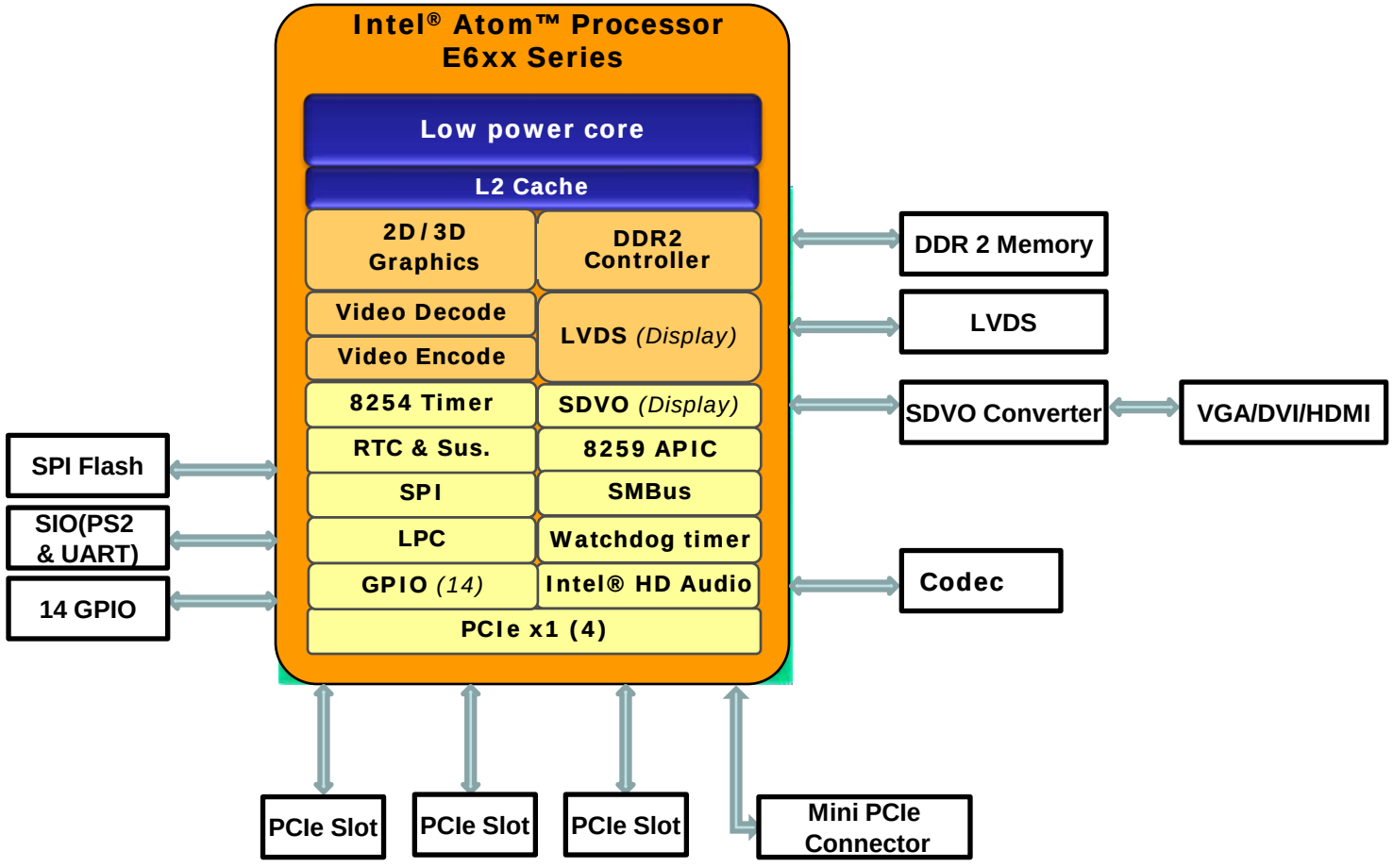
4 x1 PCI Express* Gen1.0 Ports

Intel® Atom™ E6xx Series integrates Processor, GMCH and ICH

PCIe: PCI Express* Technology

IDF2011 INTEL DEVELOPER FORUM

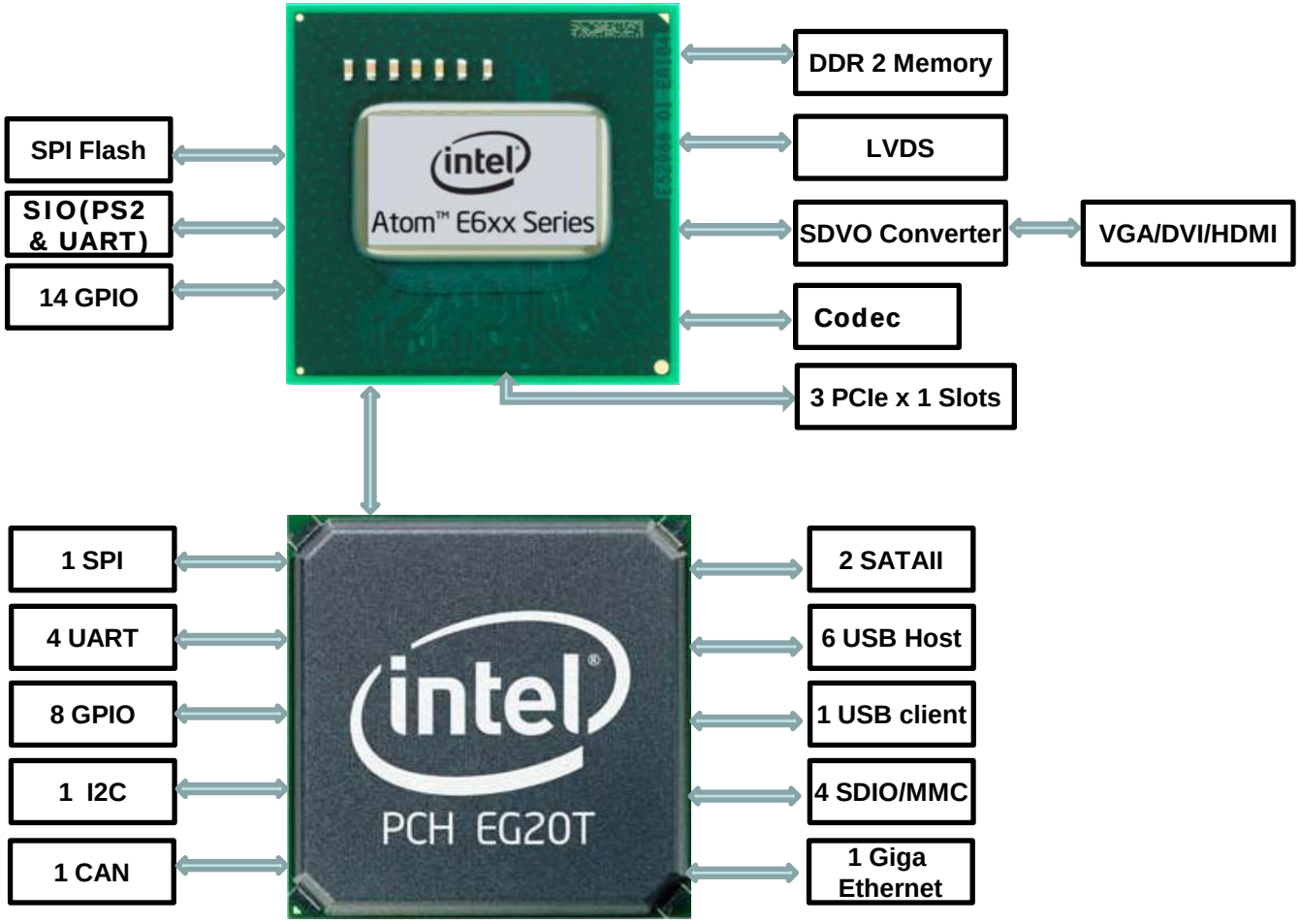
Build Single Chip System with Intel® Atom™ Processor E6xx Series



Intel® Atom™ E6xx Series are a complete system by itself

PCIe: PCI Express* Technology

CRB Diagram of Intel® Atom™ Processor E6xx Series with Intel® PCH EG20T



Intel® Atom™ Processor E6xx Series-based Platform for General Embedded Purposes

PCH:Platform Controller Hub
CRB: Customer Reference Board

IDF2011
INTEL DEVELOPER FORUM

Firmware requirements of the CRB

- Support all SKUs of the Intel® Atom™ processor E6xx series
- Support updating the firmware image on the SPI flash
- Support loading EFI Option Rom on devices connected to the PCI/PCIe ports
- Support the ACPI 3.0 states
- Support Booting from SPI flash, USB, SATA, SD, PXE, CD/DVD
- Support booting to Windows* CE 6.0, MeeGo* 1.1 and Fedora* 13
- Support to **scale** to other system
- Support feature **configuration**
- Support to **boot** to the OS loader within 2000 milliseconds
- Support to present the **splash screen** within 1.0 second

Use Intel® UDK2010 to achieve these goals

CRB: Customer Reference Board; PCIe: PCI Express* Technology; Intel® UDK2010: Intel® UEFI Development Kit 2010

Develop the SoC Advanced Features

Scalable

Scale firmware for fragment Intel® Atom™ E6xx based platforms

Configurability

Customize the platform with PCD

Performance

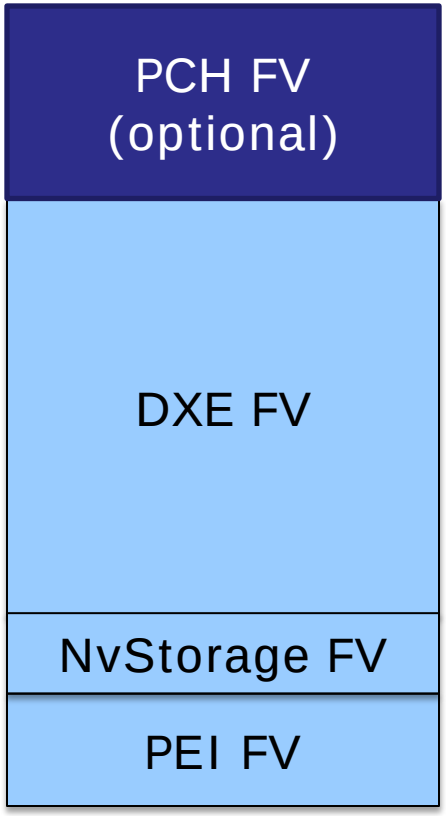
How make Intel Atom E6xx based platform boot fast

Splash Screen

How to present splash screen earlier

IDF2011
INTEL DEVELOPER FORUM

SoC Firmware Flash Layout Organization



- FD (Flash Device image) sections can be customized
- The PCH drivers are gathered in a FV, PCH FV
- Drivers in other FVs have no dependency to drivers in PCH FV

Easy to scale to different Intel® Atom™ E600 platforms

IDF2011
INTEL DEVELOPER FORUM

Develop the SoC Advanced Features

Scalable

Scale firmware for fragment Intel® Atom™ E6xx based platforms

Configurability

Customize the platform with PCD

Performance

How make Intel Atom E6xx based platform boot fast

Splash Screen

How to present splash screen earlier

IDF2011
INTEL DEVELOPER FORUM

Configurable - PCD Introduction

- Platform Configuration Database (PCD) is an important feature of Intel® UDK2010
- Platform level PCD file describes the content of the build for a specific platform
- PCDs can be used to store Platform Information
  - Vital Produce Data (VPD)
  - Setup Options
  - Serial Number
  - …

Using PCD can centralize platform configuration items

IDF2011 INTEL DEVELOPER FORUM

PCD Implementation for CRB

- More than 400 PCDs are exposed

  - Pre-allocated memory for IGD
  - Internal Device Enable
  - PCI Express* Root Port Configuration
  - Processor Power Management
  - SMBIOS configurations
  - BDS related configuration including boot order
  - ACPI PCI Routing
  - ACPI MADT
  - Process features switch
  - Others

- The PCD setting can be changed in either source code or binary image

PCD configuration makes the firmware workable on similar platforms

IDF2011
INTEL DEVELOPER FORUM

Develop the SoC Advanced Features

Scalable

Scale firmware for fragment Intel® Atom™ E6xx based platforms

Configurability

Customize the platform with PCD

Performance

How make Intel Atom E6xx based platform boot fast

Splash Screen

How to present splash screen earlier

IDF2011
INTEL DEVELOPER FORUM

Boot Performance Enhancement for SoC

Some tips to tune boot performance

- Minimize code/data access without cache
- Minimize flash region access, organize flash layout effectively
- Hardcode some parameters (i.e. memory solder down)
- Remove interaction UI
- Connect less devices
- Cooperate with OSV, reduce duplicate work between firmware and Operation System

More details in a whitepaper located at: http://edc.intel.com/Link.aspx?id=4603

UI: User Interface
OSV: Operation System
SoC: System-on-Chip

Develop the SoC Advanced Features

Scalable

Scale firmware for fragment Intel® Atom™ E6xx based platforms

Configurability

Customize the platform with PCD

Performance

How make Intel Atom E6xx based platform boot fast

Splash Screen

How to present splash screen earlier

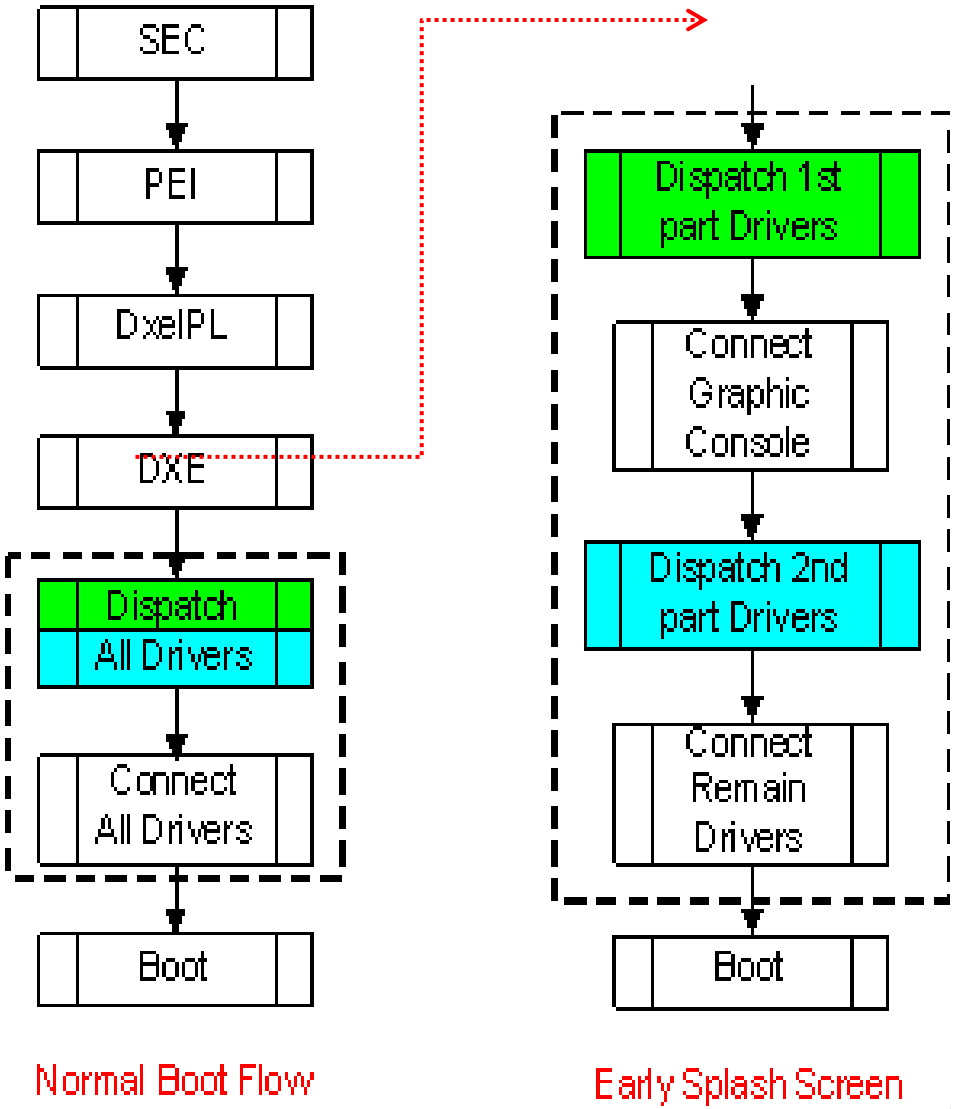
Splash Screen

- Change the boot flow to make splash screen present earlier
- Move part of drivers to another FV to reach this goal

Time Comparison

	Normal Boot	Early Splash Screen
Time[1]	1200 ms	980 ms

[1]The Time is from power on to showing screen



Normal Boot Flow

Early Splash Screen

IDF2011
INTEL DEVELOPER FORUM

Agenda

- Why use Intel® UEFI Development Kit 2010 (Intel® UDK2010) in System-On-Chip (SoC)
- Enable Intel® Atom™ Processor E6xx with Intel® UDK2010
- **Byosoft* SoC Boot Loader Development**

Byosoft* SoC Boot Loader Development

- For Byosoft*, the boot loader solution for Intel® Architecture (IA) based SoC design is a key business area
- Leverage the advantages of Intel® UDK2010 for SoC designs
  - Reuse the function modules of other platforms
  - Develop new features based on the Intel UDK2010
    - IPv6 Network Stack
    - Security Framework
    - Library instances
    - Platform Configuration Database (PCD)

Intel® UDK2010 can accelerate the SoC boot loader development

IDF2011 INTEL DEVELOPER FORUM

Byosoft* SoC Boot Loader Development

- For different market requirements, Byosoft has different solutions

IDF2011 INTEL DEVELOPER FORUM

Identity Authentication Solution

- Byosoft* Identity Authentication Solution is to solve pirated designs

Identity Authentication Solution

Encrypt customer information to generate license key

Authenticate the license status

Automatically lock the non-licensed products to stop the infringement

IDF2011
INTEL DEVELOPER FORUM

Identity Authentication Solution

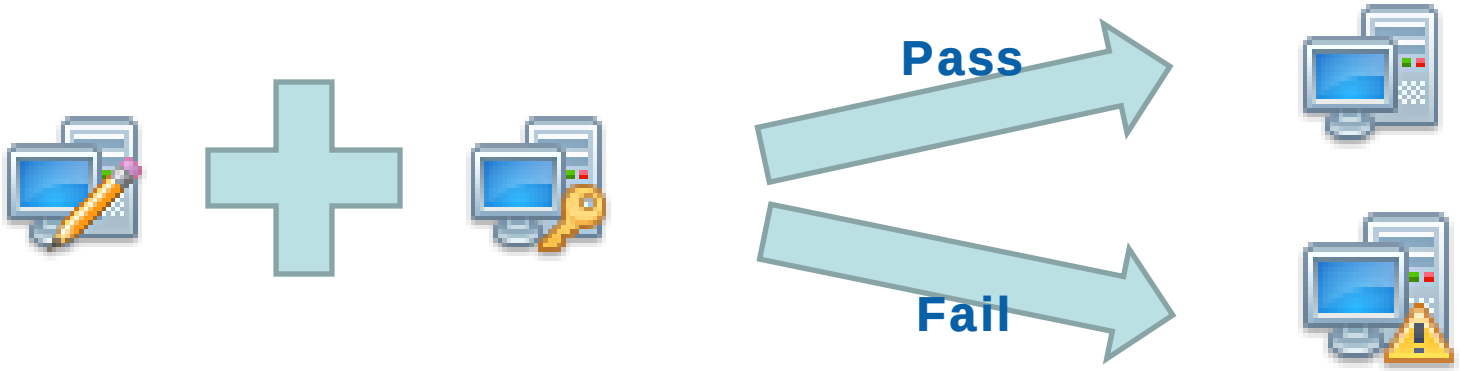
Work flow of the initial phase in the boot loader

- ✓ Assign license key
- ✓ Based on license key to generate a new key through encryption module
- ✓ Save the new key into flash

IDF2011
INTEL DEVELOPER FORUM

Identity Authentication Solution

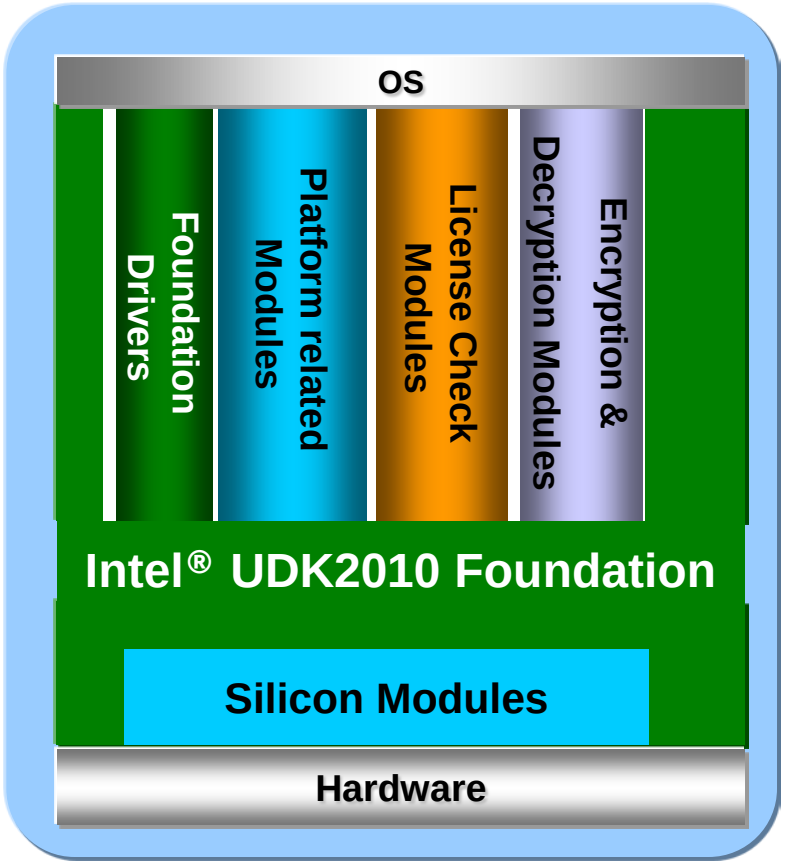
Work flow of the execution phase in the boot loader



- ✓ Check the information of hardware & boot loader
- ✓ Check the license key through the decryption module
- ✓ Pass the authentication and boot the system normally
- ✓ Or, lock the non-licensed products and notice the customer

IDF2011
INTEL DEVELOPER FORUM

Identity Authentication Solution



- License Check Module - Customized credential provider under standard UEFI/UDK PBA Framework for platform authentication and identification
- Flexible key deployment & Derivation mechanism based on UEFI Key Management Service Protocol

Take full advantage of Intel® UDK2010 Security Infrastructure

Intel® UDK2010: Intel UEFI Development Kit 2010

IDF2011 INTEL DEVELOPER FORUM

Error Report & Recovery Solution

- Byosoft* Error Report & Recovery Solution is used in Industry Control system

Error report & recovery solution

Report the error info through network in security way

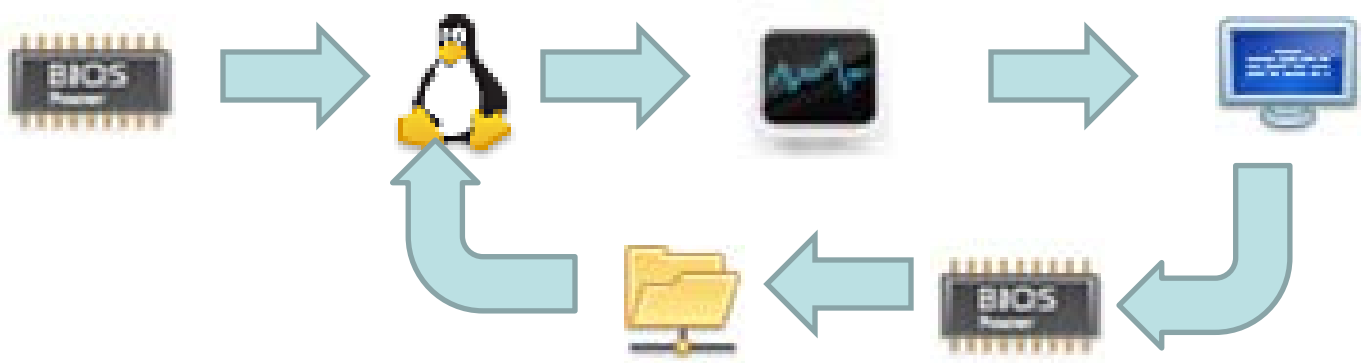
Recovery the system if detects errors

Keep the system stable

IDF2011
INTEL DEVELOPER FORUM

Error Report & Recovery Solution

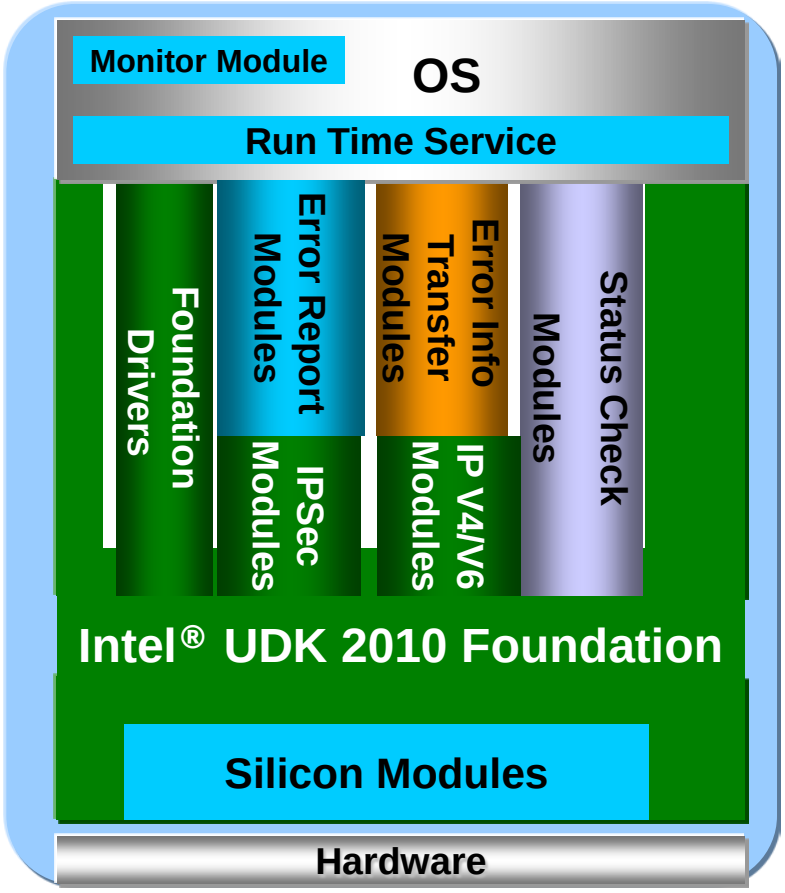
Work flow of error handling



- ✓ Boot to OS
- ✓ Monitor System Status
- ✓ System meets error
- ✓ Recover the system
- ✓ Upload error information to the server
- ✓ Back to the normal state

IDF2011
INTEL DEVELOPER FORUM

Error Report & Recovery Solution



- Error Info Transfer Module - Leverage Intel® UDK2010 IPV4/IPV6 stack to transfer error report
- Error Report Module - The error report is encrypted by Intel® UDK2010 IP Sec module.
- Use UEFI Runtime service to communicate between OS and firmware

Develop advanced features based on Intel® UDK2010 network fundamental components

Intel® UDK2010: Intel UEFI Development Kit 2010

IDF2011 INTEL DEVELOPER FORUM

Fast Boot Solution

- Byosoft* Fast Boot Solution is used in the devices which have strict boot performance requirements

Fast Boot Solution

Only enable necessary devices

Improve the efficiency of code execution by making full use of cache

Use the fixed boot mode according the usages of the device

IDF2011
INTEL DEVELOPER FORUM

Fast Boot Solution

- The core of Intel® UDK2010 is modular making it more efficient to optimize
- Intel® UDK2010 supports to integrate all required drivers into one FV image to save decompressing time
- It is easy to save and reuse data to avoid long time enumeration and hardware training in Intel® UDK2010
- Byosoft* can customize the boot loader to satisfy different requirements from customers

The architecture of Intel® UDK2010 supports performance tuning

Intel® UDK2010: Intel UEFI Development Kit 2010

Fast Boot Solution

- Boot performance comparison between Normal Boot and Fast Boot

Boot Phase	Normal Boot Performance	Fast Boot Performance
SEC	12 ms	16 ms
PEI	1592 ms	516 ms
DXE	594 ms	207 ms
BDS	13594 ms	1623 ms
Total Time	15792 ms	2362 ms

IDF2011
INTEL DEVELOPER FORUM

Summary

- Intel® UDK2010 naturally supports SoC boot loader development
- Based on Intel® UDK2010, Byosoft makes the innovation for SoC boot loader
- Byosoft* will continue to commit itself on SoC boot loader service and development

Additional resources on UEFI:

- Other UEFI Sessions – Next slide
- More web based info:
  - Specifications sites www.uefi.org, www.intel.com/technology/efi
  - EDK II Open Source Implementation: www.tianocore.org

- Technical book from Intel Press: "Beyond BIOS: Implementing the Unified Extensible Firmware Interface with Intel's Framework" www.intel.com/intelpress

EFI Track Sessions

Session ID	Title	Day/ Time	Room
✓EFIS001	Microsoft* Windows* Platform Evolution and UEFI	Tuesday 11:10	306A
✓EFIS002	UEFI Development and Innovations for System-On-Chip (SoC)	Tuesday 14:05	306A
EFIS003	UEFI and Transparent Computing Technology	Tuesday 15:10	306A
EFIS004	Intel® UEFI Development Kit 2010 and Intel® Boot Loader Development Kit: Foundations for Advanced Embedded Development	Tuesday 16:10	306A
SPCQ001	Hot Topic Q&A: Intel® Boot Loader Development Kit (Intel® BLDK)	Tuesday 17:00	306A
EFIS005	Security and Networking Advancements Today's UEFI and Intel® UEFI Development Kit 2010 (Intel® UDK2010)	Wednesday 11:10	306A

✓ = DONE

IDF2011 INTEL DEVELOPER FORUM

Session Presentations - PDFs

The PDF for this Session presentation is available from our IDF Content Catalog at the end of the day at:

intel.com/go/idfsessionsBJ

URL is on top of Session Agenda Pages in Pocket Guide

Please Fill out the Session Evaluation Form

Give the completed form to the room monitors as you exit!

Thank You for your input, we use it to improve future Intel Developer Forum events

Q&A

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 PROPETY 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 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.
- Tunnel Creek 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
- 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, Atom, Atom inside, Sponsors of Tomorrow. 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.
- Copyright ©2011 Intel Corporation.

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. 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 corporation's expectations. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions; 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. 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 impacted 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 September 25, 2010.

Rev. 1/13/11