片上系统（SoC）的 UEFI 开发与创新特性

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

EFIS002
• 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
• 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.
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
The Intel® UDK2010 is an open source build environment and tools that supports the development of UEFI Firmware, drivers and applications.

- Netbooks
- Smartphones
- TVs
- Embedded: Auto, Signage, Printers, etc.
- Gadgets
- Networks
- Data Center / Servers
- Desktop PCs
- Notebooks

Intel® UDK2010 Enables a Common Firmware Development Foundation Across the Compute Continuum
**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**
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
• 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**
Build Single Chip System with Intel® Atom™ Processor E6xx Series

Intel® Atom™ E6xx Series are a complete system by itself
CRB Diagram of Intel® Atom™ Processor E6xx Series with Intel® PCH EG20T

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

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

<table>
<thead>
<tr>
<th>Normal Boot</th>
<th>Early Splash Screen</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time</strong>&lt;sup&gt;1&lt;/sup&gt;</td>
<td>1200 ms</td>
</tr>
</tbody>
</table>

<sup>1</sup>The Time is from power on to showing screen
• 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
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.
Byosoft* SoC Boot Loader Development

• For different market requirements, Byosoft has different solutions

Identity Authentication Solution
Error report & recovery solution
Fast Boot Solution

Intel® Atom™ Processor E6xx Series based on Intel® UDK2010
Identity Authentication Solution

- Byosoft* Identity Authentication Solution is to solve pirated designs

  Encrypt customer information to generate license key

  Authenticate the license status

  Automatically lock the non-licensed products to stop the infringement
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
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
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
Error Report & Recovery Solution

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

- Report the error info through network in security way

- Recovery the system if detects errors

- Keep the system stable
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
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
Fast Boot Solution

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

- 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
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.
Fast Boot Solution

- Boot performance comparison between Normal Boot and Fast Boot

<table>
<thead>
<tr>
<th>Boot Phase</th>
<th>Normal Boot Performance</th>
<th>Fast Boot Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC</td>
<td>12 ms</td>
<td>16 ms</td>
</tr>
<tr>
<td>PEI</td>
<td>1592 ms</td>
<td>516 ms</td>
</tr>
<tr>
<td>DXE</td>
<td>594 ms</td>
<td>207 ms</td>
</tr>
<tr>
<td>BDS</td>
<td>13594 ms</td>
<td>1623 ms</td>
</tr>
<tr>
<td>Total Time</td>
<td>15792 ms</td>
<td>2362 ms</td>
</tr>
</tbody>
</table>
总结

- 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
关于UEFI的更多信息：

• 相关课程 - 下一页
• More web based info:
  – EDK II Open Source Implementation: www.tianocore.org

  www.intel.com/intelpress
<table>
<thead>
<tr>
<th>课程编号</th>
<th>课程标题</th>
<th>日期/时间</th>
<th>教室</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFIS001</td>
<td>微软* Windows*平台演进与UEFI规范</td>
<td>周二 11:10</td>
<td>306A</td>
</tr>
<tr>
<td>EFIS002</td>
<td>片上系统（SoC）的 UEFI 开发与创新特性</td>
<td>周二 14:05</td>
<td>306A</td>
</tr>
<tr>
<td>EFIS003</td>
<td>UEFI 和透明计算技术</td>
<td>周二 15:10</td>
<td>306A</td>
</tr>
<tr>
<td>EFIS004</td>
<td>英特尔® UEFI 开发套件 2010 和英特尔® Boot Loader 开发套件：高级嵌入式开发基础</td>
<td>周二 16:10</td>
<td>306A</td>
</tr>
<tr>
<td>SPCQ001</td>
<td>热点问题问答：英特尔® Boot Loader 开发套件（英特尔® BLDK）</td>
<td>周二 17:00</td>
<td>306A</td>
</tr>
<tr>
<td>EFIS005</td>
<td>当前 UEFI 和英特尔® UEFI 开发套件 2010（英特尔® UDK2010）在安全性和网络连接方面的进展</td>
<td>周三 11:10</td>
<td>306A</td>
</tr>
</tbody>
</table>

✓ = 完毕
本课程演示文稿 - PDFs

本课程演示文稿 （PDF） 发布在技术课程目录网站：

intel.com/go/idfsessionsBJ

该网址同时打印于会议指南中专题讲座日程页的上方
请填写课程评估表

请将您填写完的课程评估表交予大会工作人员

非常感谢您的反馈，我们将据此改进未来的英特尔信息技术峰会
问答
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 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.
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.