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

顾晓刚，开发经理，英特尔
晋磊，技术市场工程师，英特尔

EFIS004

英特尔®与你共创明天™ intel

议程

- Intel® UDK2010 的主要特点
- 嵌入式设备的启动引导程序
- Intel® BLDK 的主要特点
- 总结

议程

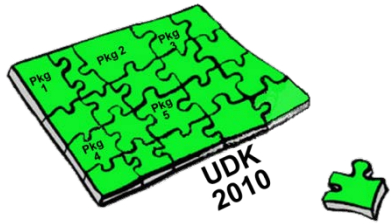
- Intel® UDK2010 的主要特点
- 嵌入式设备的启动引导程序
- Intel® BLDK 的主要特点
- 总结

Intel® UDK2010 适用于各类计算设备固件开发

Intel® UDK2010 的主要特点

- 遵循UEFI规范
- 灵活的包管理机制
- 支持多种编译器和操作系统
- 平台配置数据库(PCD)
- 优化的库函数
- 内嵌源代码调试工具
- 增强的安全支持
- 支持IPv6网络

支持UEFI规范



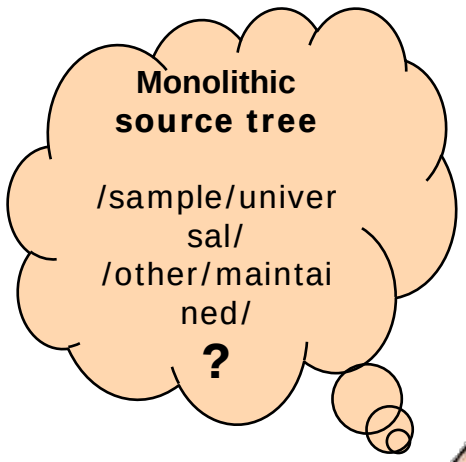
- Intel® UDK2010 原生支持:
  - 支持最新的 UEFI 2.2, UEFI 2.3, PI 1.1和PI 1.2规范（同时兼容以前各版本的UEFI, EFI和PI 规范)
    - 在单独的Shell包中支持Shell 2.0规范
  - Pre-UDK 包括所有 UEFI 2.0, UEFI 2.1, PI 1.0 and Framework 0.9x 规范的定义 (PEI Core, DXE Core, PEIMs, DXE驱动程序, UEFI驱动程序和库函数)

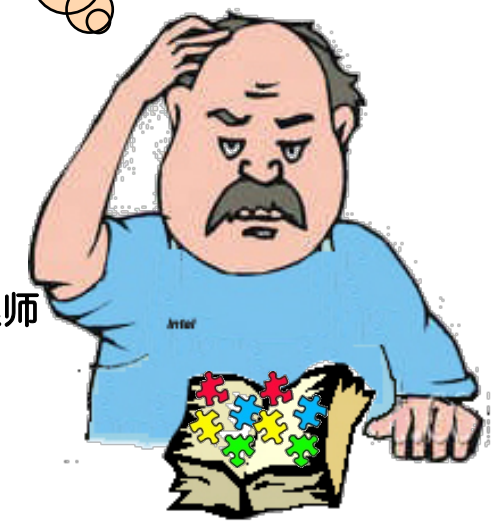
安全和网络 - UEFI 2.3
- IPV6/IPSec – 下一代互联网IP地址的分配及网络安全
- 用户认证和驱动程序签名
- iSCSI & VLAN

Human Infrastructure Interface (HII) – UEFI 2.1

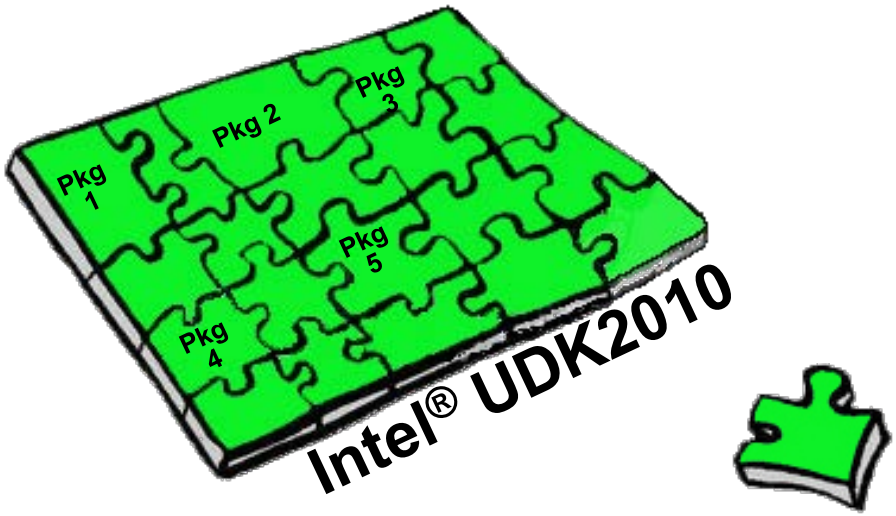
基于高级工业规范的特性

包管理：有利于高级功能的快速交付





固件开发工程师

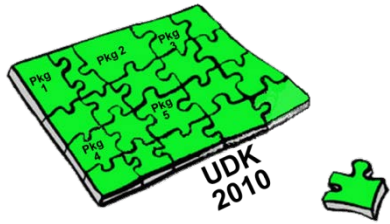


基于包的部署实例

- **Package 1** 工业标准模块和驱动
- **Package 2** 芯片的PEI模块和DXE模块
- **Package 3** 板级开发代码
- **Package 4** OEM增值代码

Intel® UDK2010 方便各种模块的整合

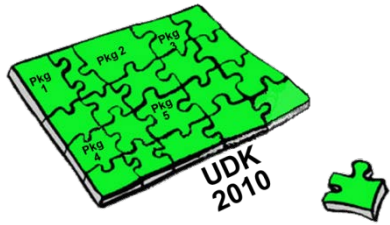
支持多种编译器和操作系统

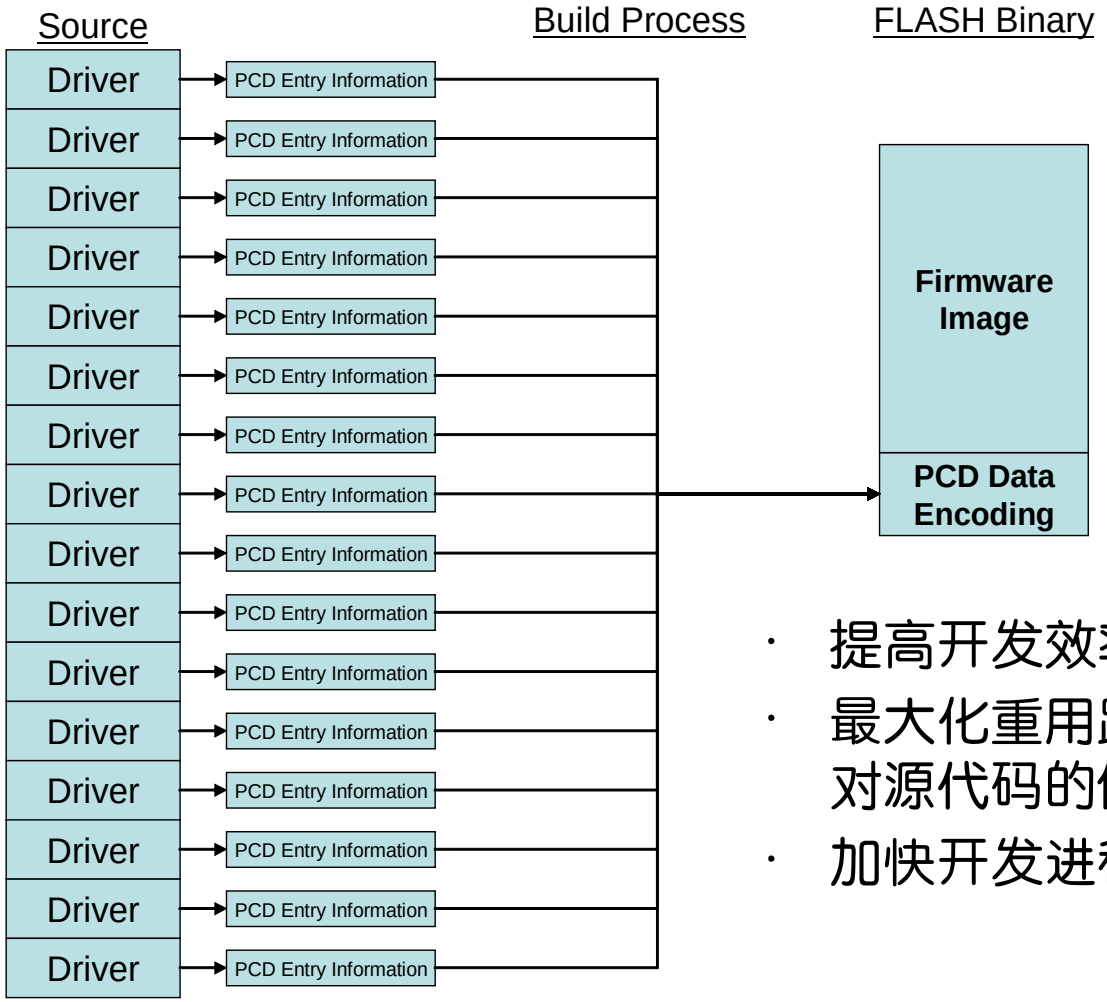


	EDK	Intel® UDK2010
操作系统	Windows* XP	Windows XP, Vista32, Vista64, Windows 7, Linux*, OS/X*
编译器、链接器	Visual Studio 2003, 2005, WinDDK	Visual Studio 2003*, 2005*, 2008*, WinDDK*, Intel® C++Compiler, GCC
Build	nmake	nmake, gmake
Build Tools	C	POSIX C, Python*

GCC GNU Compiler Collection for C++
POSIX C Portable Operating System Interface for Unix

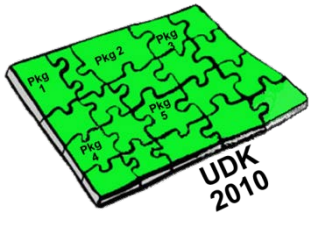
平台配置数据库

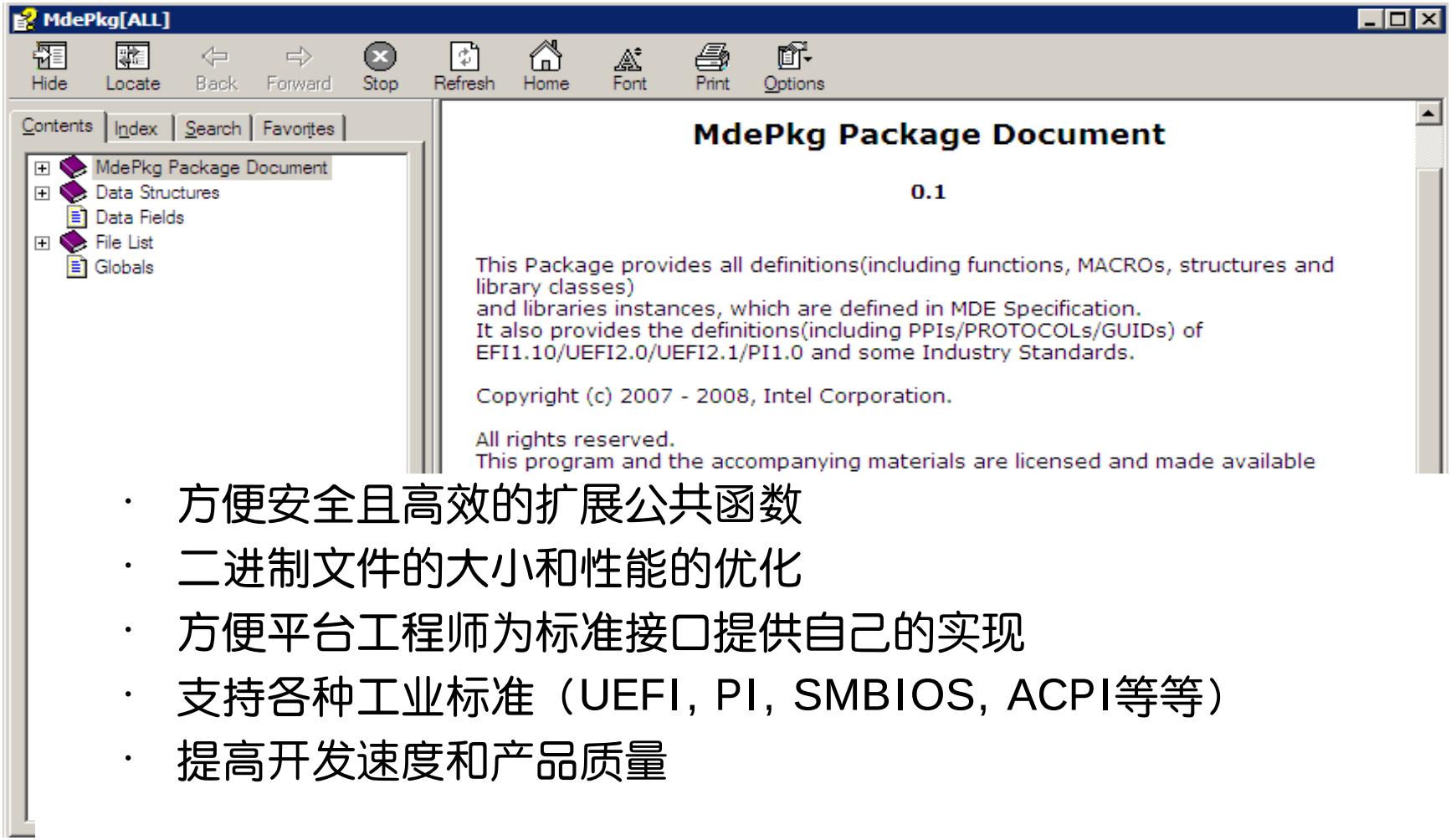




- 提高开发效率
- 最大化重用跨平台代码，最小化对源代码的修改
- 加快开发进程

优化的库函数



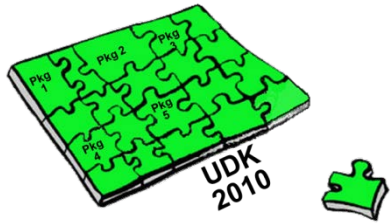


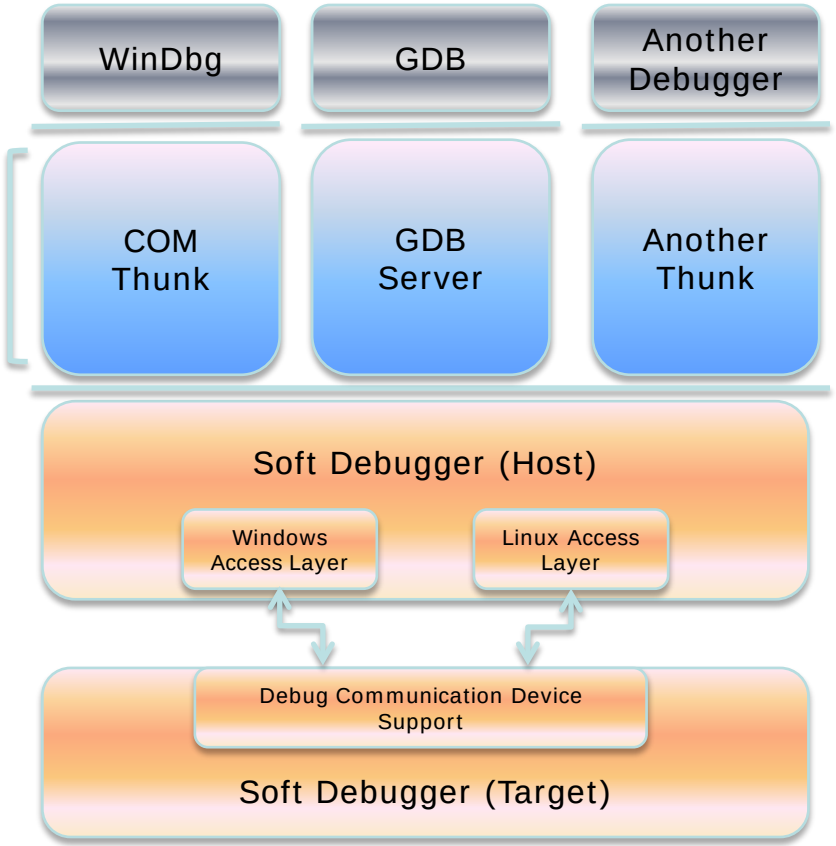
- 方便安全且高效的扩展公共函数
- 二进制文件的大小和性能的优化
- 方便平台工程师为标准接口提供自己的实现
- 支持各种工业标准（UEFI，PI，SMBIOS，ACPI等等）
- 提高开发速度和产品质量

源代码调试

Intel® UDK2010 包含源代码调试工具：

- 类似于标准的Windows* WinDBG* 工具
  - 易学习
  - 功能强大
  - 支持早期预启动阶段的调试
- 直接集成于平台的预启动映像文件
- 使用串口和USB作为与开发主机的通信接口





Intel® UDK2010 可在www.tianocore.org 获得

tianocore.org

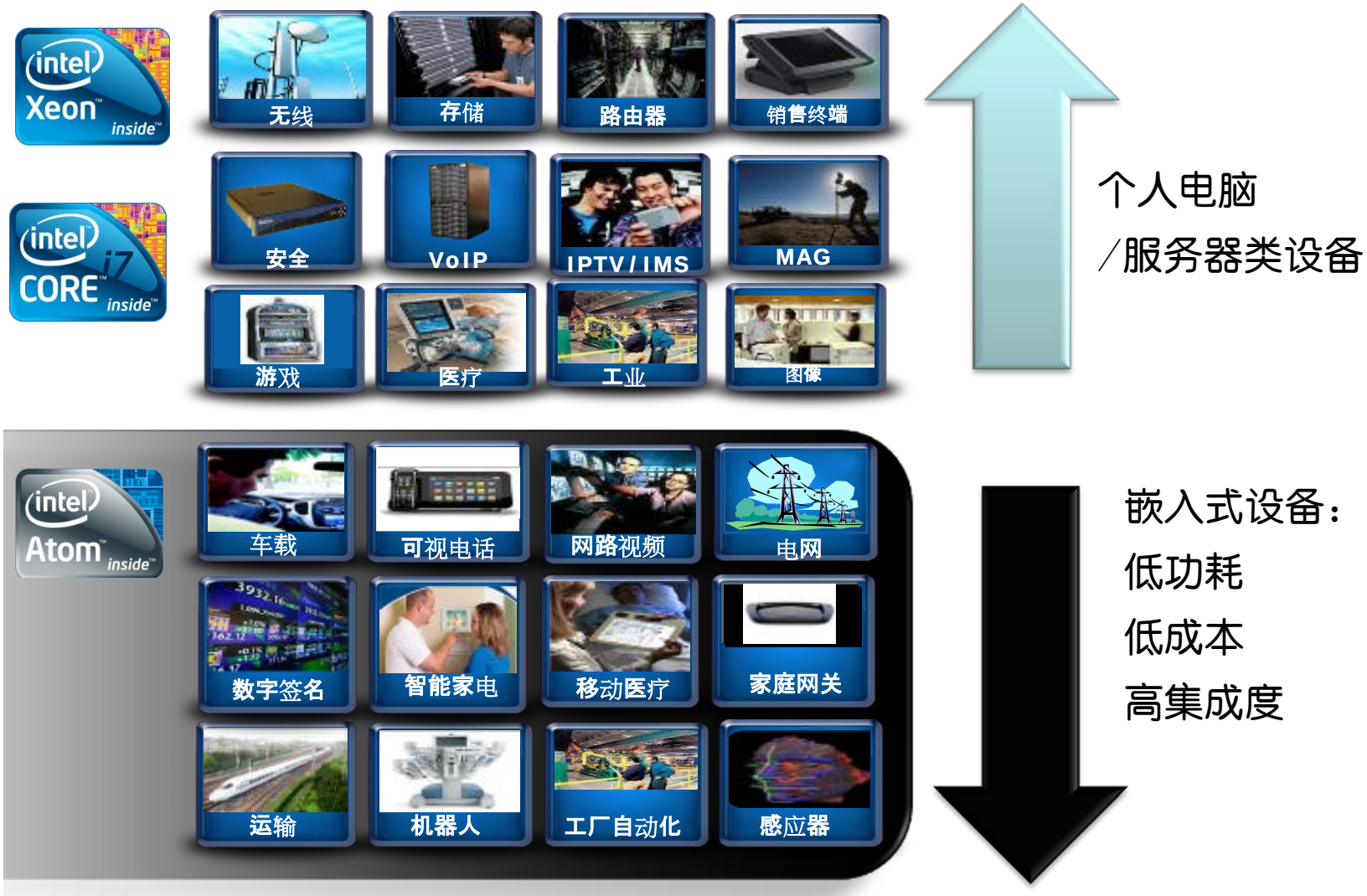
Intel® UDK2010
Open Source
UEFI Development Kit

Develop. Contribute. Advance.

议程

- Intel® UDK2010 的主要特点
- 嵌入式设备的启动引导程序
- Intel® BLDK 的主要特点
- 总结

嵌入式领域发展的现状与展望



嵌入式设备在各式各样的应用领域得到飞速发展

传统BIOS和嵌入式领域Boot Loader

BIOS
根据个人电脑工业标准进行动态配置

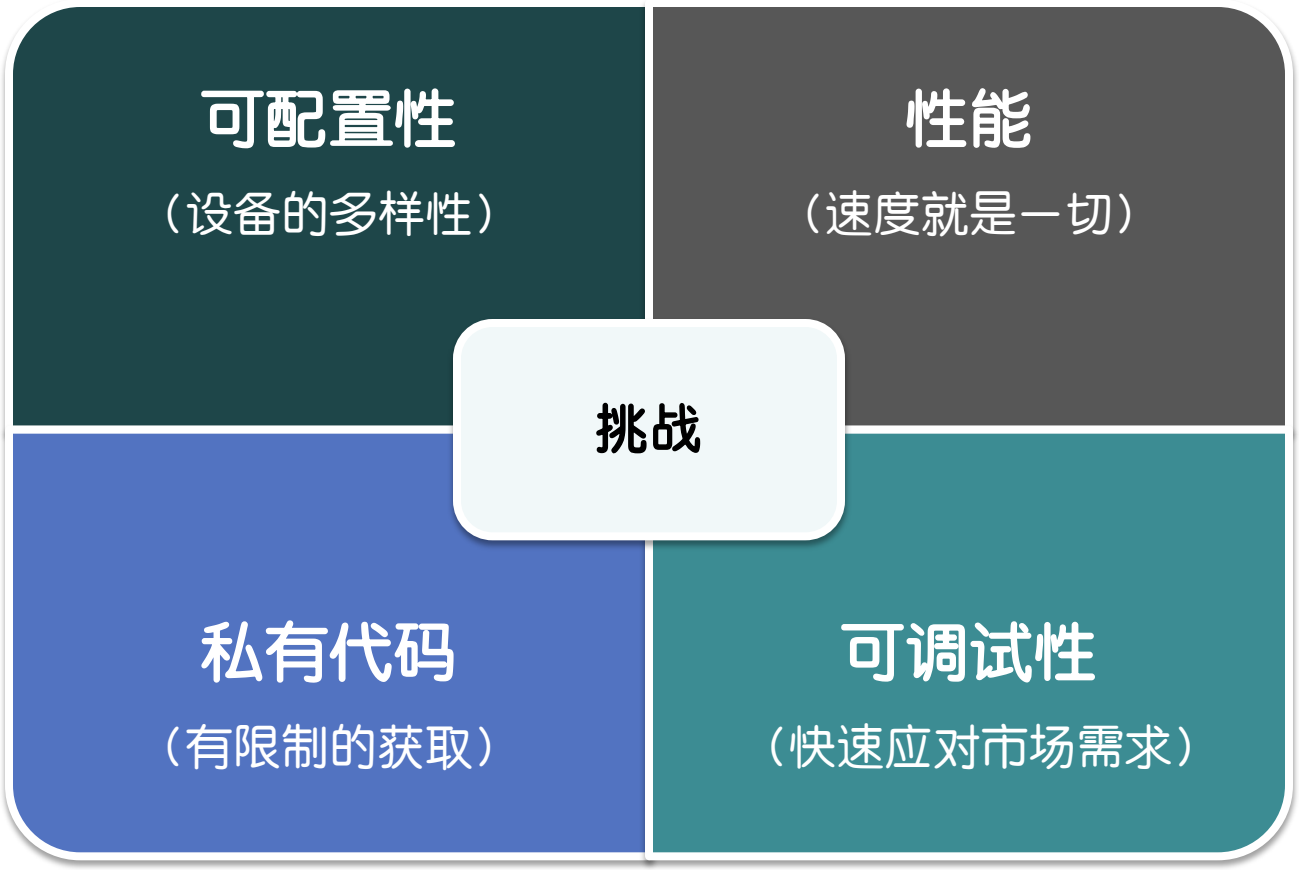
- 兼容标准的操作系统
- 具有丰富的功能特性
- 适用于大多数的应用场景
- 支持多种启动路径
- 可获得额外的技术支持和服务
- 需要付费

Boot Loader
针对一种特定的应用进行静态配置

- 定制化的操作系统和应用程序
- 提供最基本的IA架构的初始化
- 快速且精巧
- 适用于单一应用场景
- 支持特定的启动路径
- 无需炫目的配置界面
- 无需深度的技术支持
- 免授权费

Intel® BLDK 可将使用模型
从传统 BIOS扩展到嵌入式领域 Boot Loader

嵌入式设备的启动引导程序面临的挑战



Intel® UDK2010 能够帮助您应对嵌入式领域的挑战

议程

- Intel® UDK2010 的主要特点
- 嵌入式设备的启动引导程序
- Intel® BLDK 的主要特点
- 总结

Intel® BLDK 的组成元素

技术文档

- 易于理解的指导性文档可以帮助客户自我学习
- 高效、可扩展的技术支持的方法

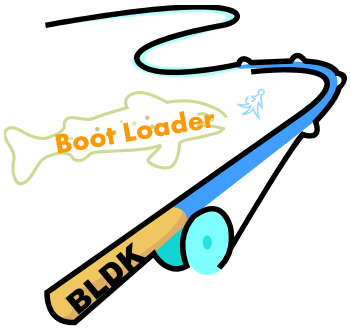
CRB和参考固件代码

- 开发客户系统的起点

图形用户接口和工具软件

- 通过使用图形化的功能模块和编译工具，客户可以在不直接修改源代码的情况下定制启动引导程序
- 集成开发环境大大方便了代码的浏览和修改

Intel® BLDK 为客户提供了开发专属的启动引导程序的机制



关于 Intel® BLDK 的详情，请访问 http://www.intel.com/go/bldk

Intel® BLDK 的主要特点

支持各种工业标准
- UEFI 2.0, UEFI 2.1, UEFI 2.2, UEFI 2.3 and PI 1.0, PI 1.1, PI 1.2
- ACPI, USB, ATA, SMBIOS, TCP/IP等等

支持二进制文件可配置
- 无需改变任何源代码，即可选择功能特性和修改二进制文件

支持多种工具
- MSFT (VS2003, VS2005, VS2008, WinDDK), GNU (GCC), INTEL (ICC)

支持多种启动设备
- 可从以下设备启动：ATA, SSD, CF, SD, USB, FWH, SPI, iSCSI, PXE

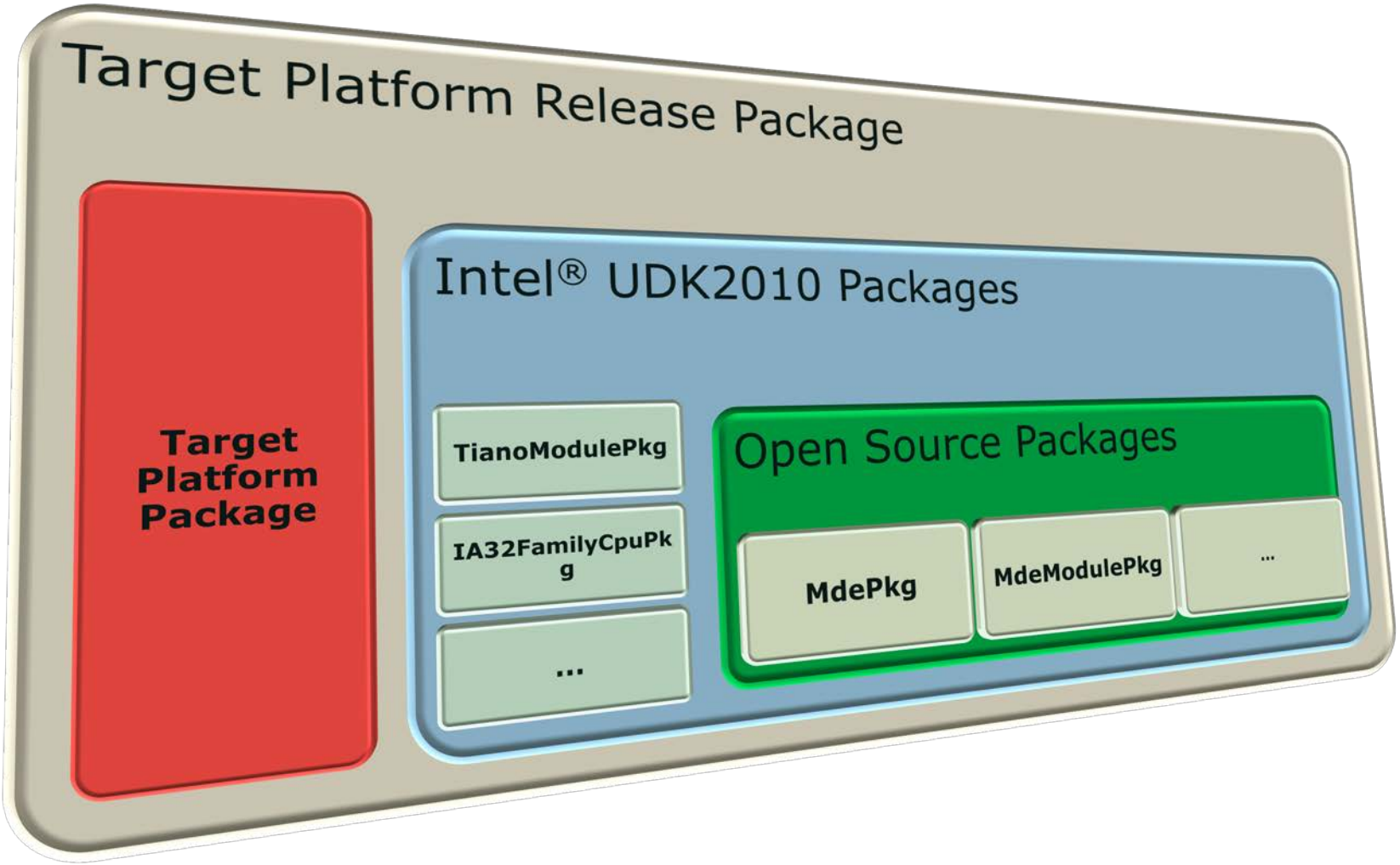
支持源代码级调试
- UDK 调试工具提供纯软件的调试方案

可扩展的基础代码
- 进入操作系统前的安全性，丰富的网络功能和管理能力等等

免授权费的源代码
- 绝大部分源代码可以从 www.tianocore.org 获得

Intel® UDK2010是嵌入式固件开发的最佳选择

配有英特尔® 凌动™ E6xx 系列处理器和英特尔® 平台控制器 EG20T的平台 – 基于Intel® UDK2010



应对挑战-可配置

- 可配置能力是嵌入式领域的关键特性
  嵌入式设备和普通个人电脑的不同在于，具有针对特定应用环境进行定制和性能进行优化的能力，这需要改变传统的行为模式。
  - 是否需要运行一个用户界面?

交互式启动

无交互式启动

  - 在运行payload之前必须初始化哪些硬件设备?

嵌入式领域通常有特定的启动策略

应对挑战-性能

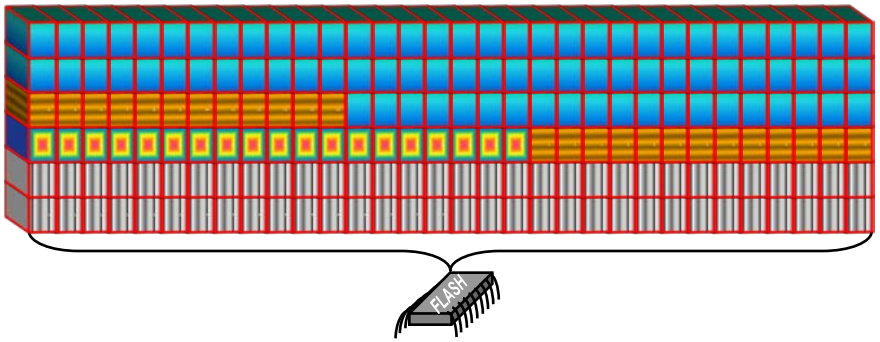
- 启动目标硬件的选择
  - 启动设备的延时影响启动性能
  - 使用固态硬盘代替传统磁盘媒质可以节省数秒的启动时间

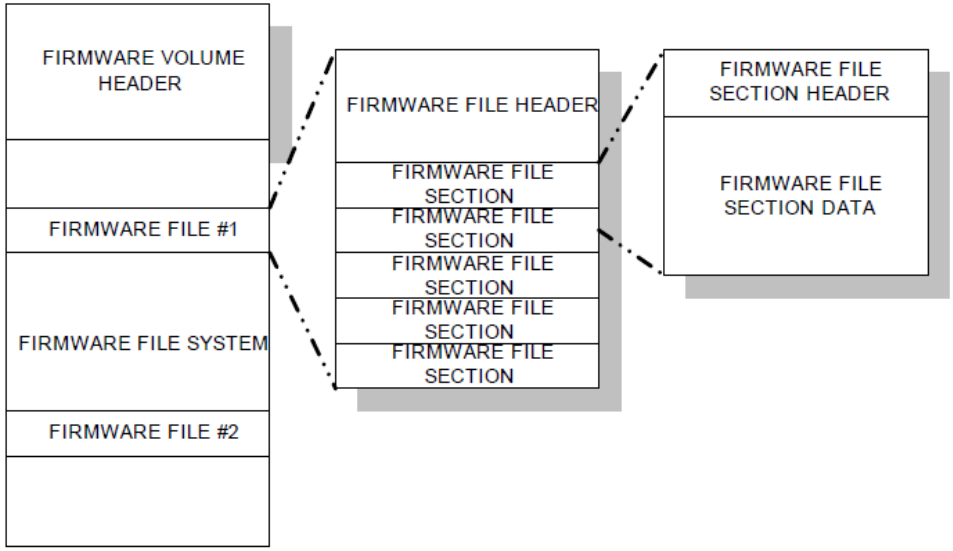
	DRAM	SSD (34nm)	EIDE
Read Latency	~30 ns	65 µs	8.5 ms
Read BW (MB/s)	1800	250	120
Write Latency	~30 ns	85 µs	10 ms
Write BW (MB/s)	1800	70	120
Spin-up/down time	N/A	N/A	1-2s++

越短的操作延时，越快的启动性能

应对挑战-性能

- FLASH的布局
  - FLASH的布局影响性能
  - 根据启动配置布局FLASH的内容，只需读取FLASH上包含启动所需核心组件模块



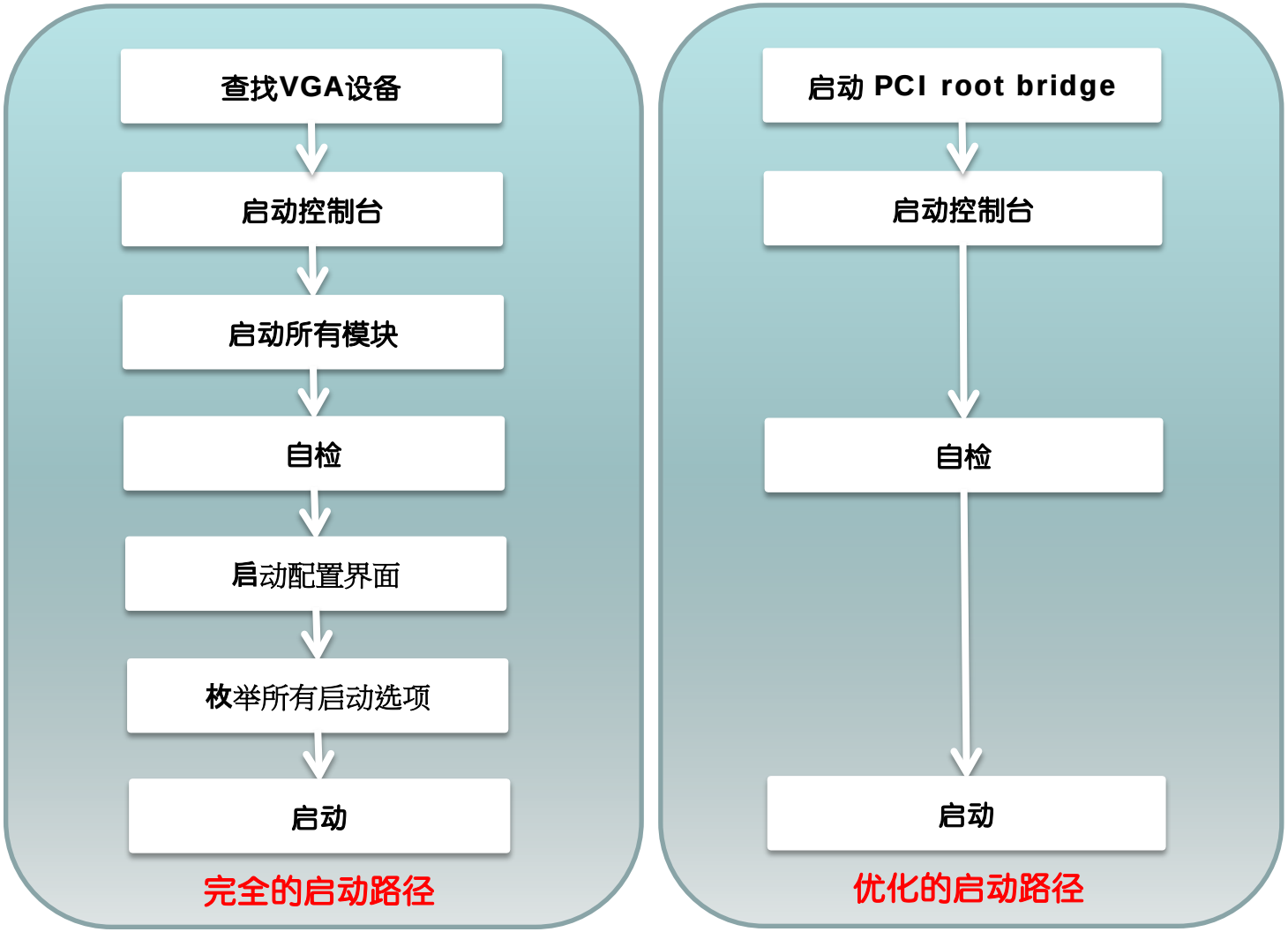


核心组件模块
数据模块
可选数据模、
空闲模块

越高效的FLASH布局，越快的启动性能

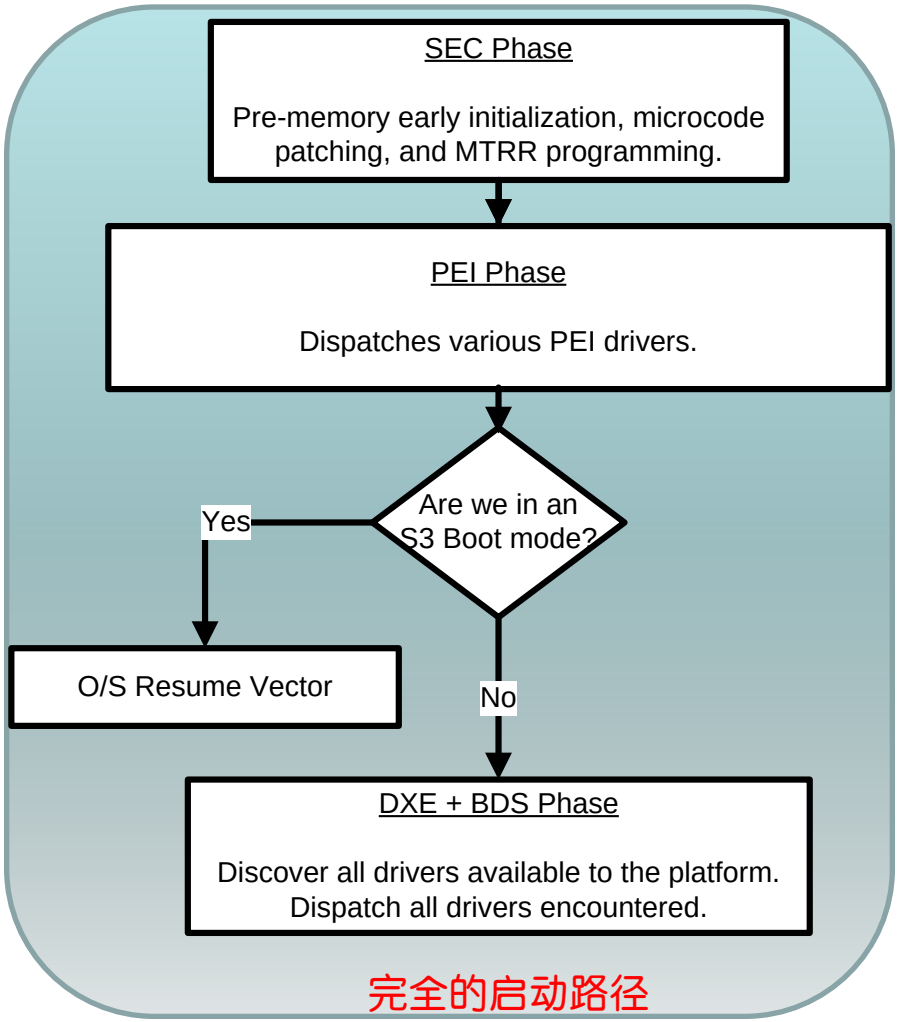
应对挑战-性能

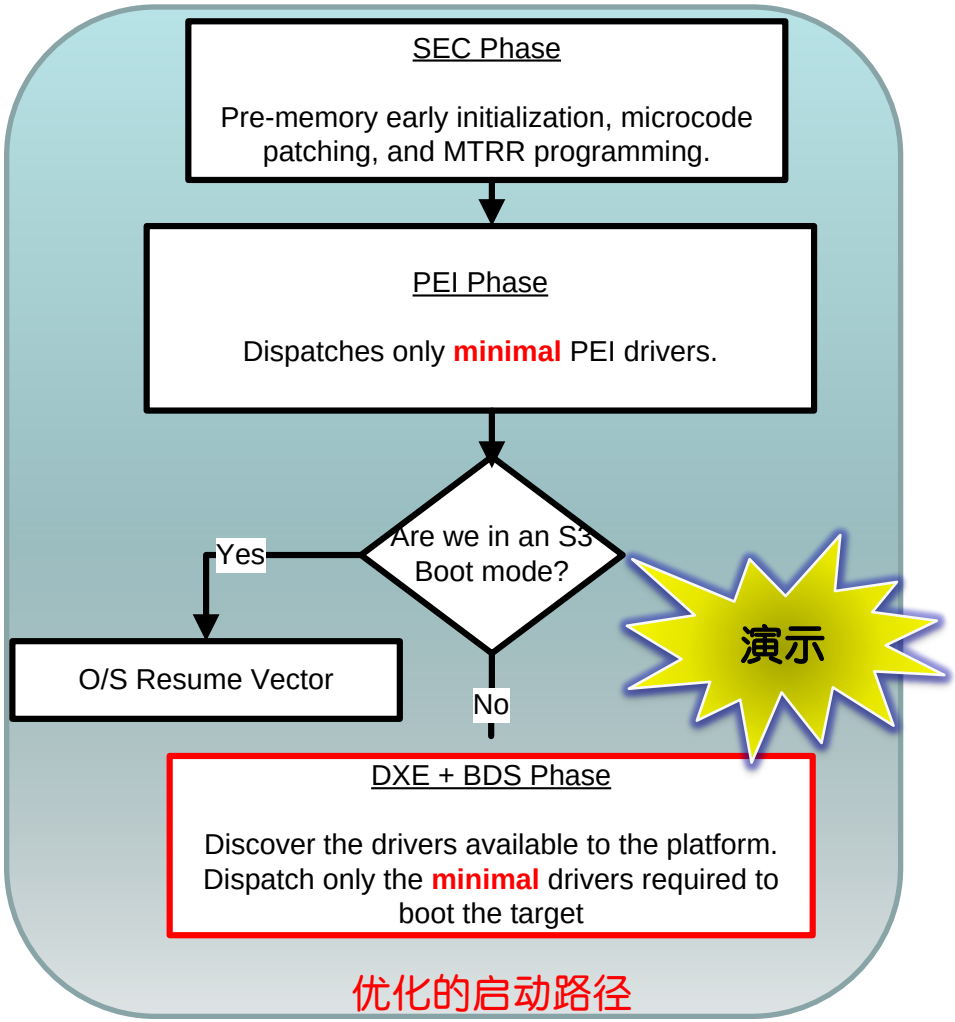
- 对于应用平台的不同需求，可以做完全不同的定制优化



越优化的模块启动顺序，越快的启动性能

应对挑战-性能



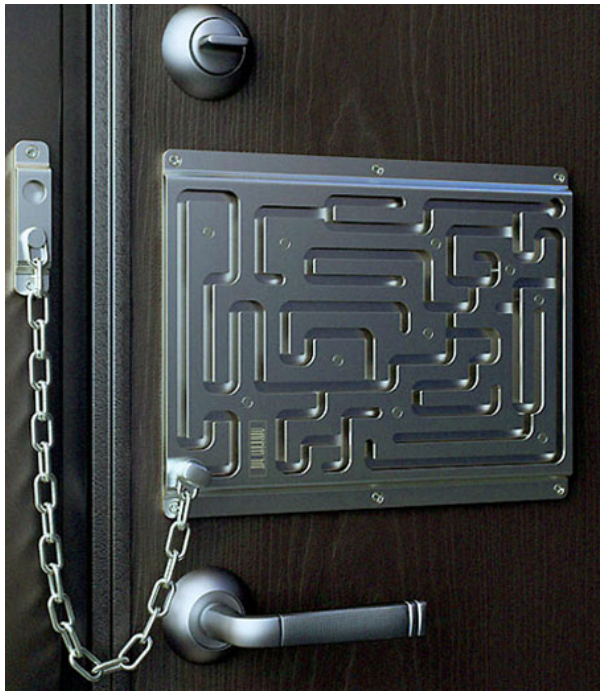


若需了解技术细节，请阅读相关白皮书：http://edc.intel.com/Link.aspx?id=4603

优化的同时保持对UEFI规范的兼容

应对挑战-私有代码

- 无法获得源代码资源
  - 传统的私有代码发布机制限制了启动引导程序源代码的获取



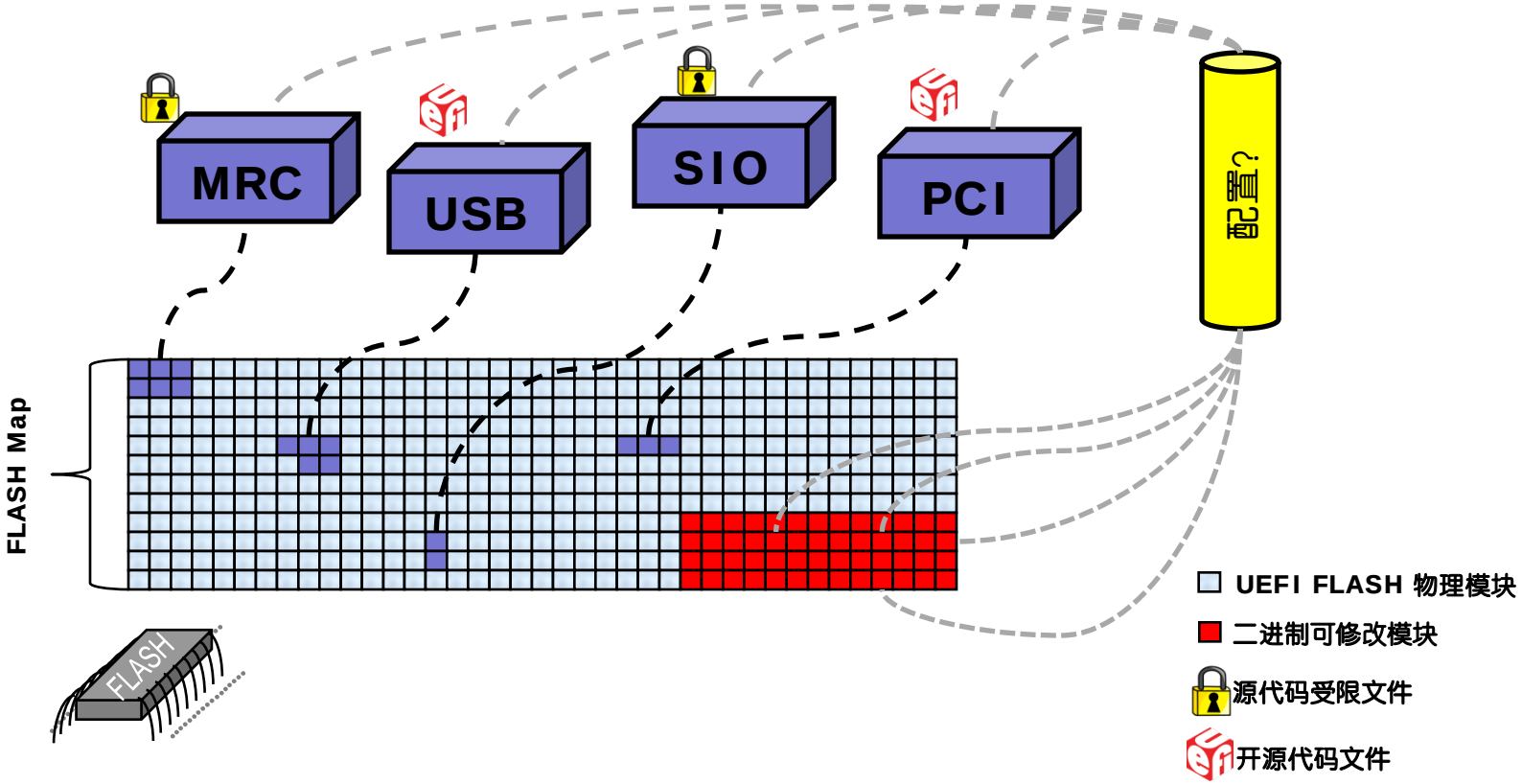
www.tianocore.org 重定向至
Source Forge repository

仅有少量受限代码

UEFI 引入了大量的开源代码

应对挑战-私有代码

- 依靠扩展二进制模块的可配置性，我们可以应对更广阔的应用场景。



对二进制文件的修改可以减少对源代码的依赖，
这种方案将被大多数用户使用

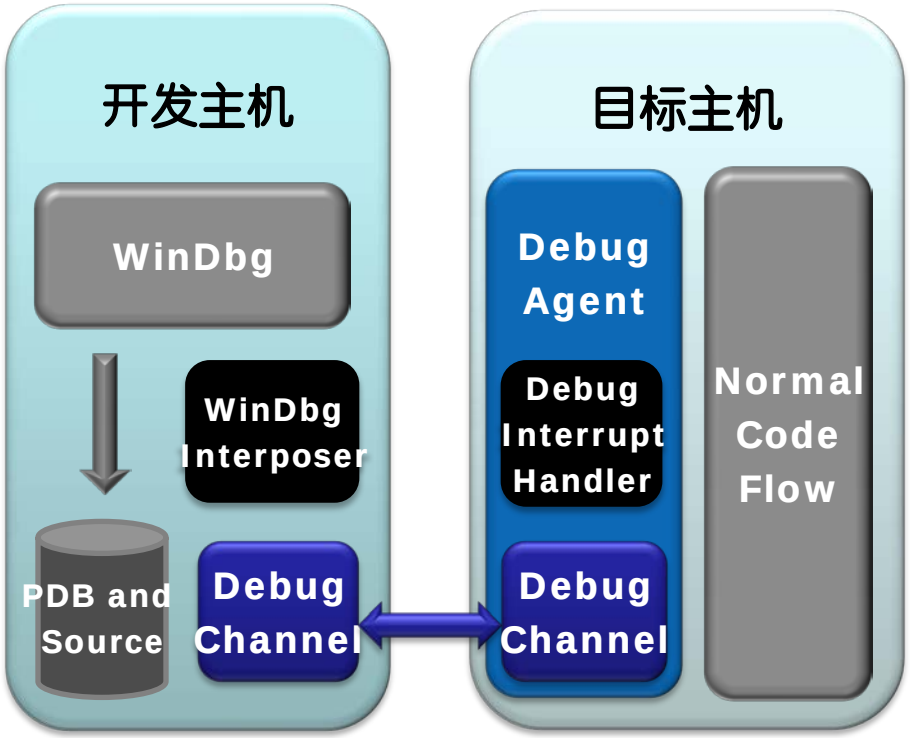
应对挑战-可调试性

- 纯软件方式的调试方案
  - 最新的Intel® UDK 调试工具（Intel® UDK Debugger Tool)
  - 无需外接JTAG接口即可进行源码调试
    - 可利用各式各样的调试端口（例如，USB和串口)
  - 使用WinDbg作为前端支持模块
  - 该调试方案几乎可以完全替代高端的硬件调试工具
    - SEC的初始代码必须预先建立堆栈
      - 通常情况下，从开机到可以调试之间有十几条指令
      - 同样，SMM 代码也要等 SMI 入口十几条指令执行完成后才可调试
    - 某些处理器模式的切换难以调试

基于UEFI的开源调试解决方案

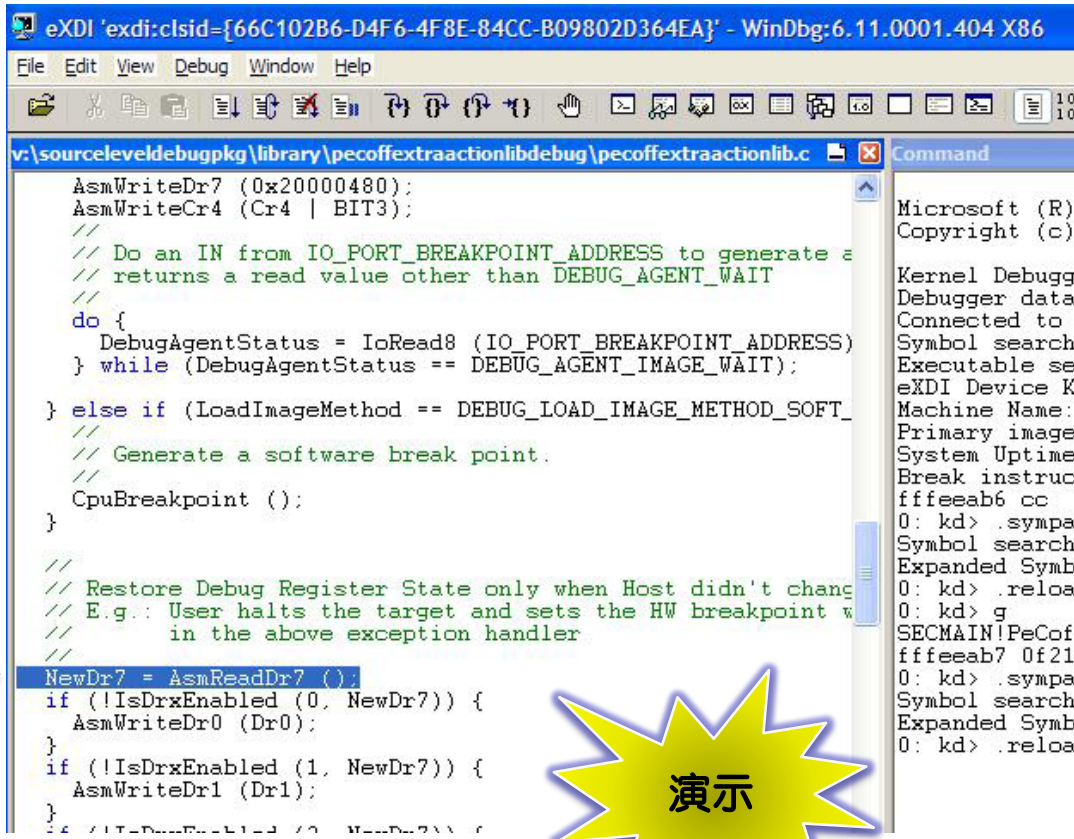
应对挑战-可调试性

- Intel® UDK Debugger Tool 的架构
  - WinDbg Interposer 解析来自WinDbg的指令
  - Debug Channel 负责开发主机和目标主机之间的通信
  - Debug Interrupt Handler 处理来自Debug Channel的命令



应对挑战-可调试性

- WinDbg 在SEC阶段的后期断下目标机器，并装载SecCore阶段的符号表，接着在如图所示窗口显示当前源代码。
- 底部窗口用来输入调试命令
  - .reboot
  - Smmentrybreak=1 or 0
  - g - Go
  - B[C|D|E][<bps>] - clear/disable/enable breakpoint(s)
  - Q - quit
  - ? – Command list



议程

- Intel® UDK2010 的主要特点
- 嵌入式设备的启动引导程序
- Intel® BLDK 的主要特点
- 总结

总结

- Intel® UDK 2010 满足了最新工业标准并提供了一套完善的开发工具和基础代码。
- Intel® BLDK 提供了基于英特尔® 凌动™处理器快速开发嵌入式领域产品的解决方案。
- Intel® UDK 2010 是能够应对嵌入式领域挑战的最佳选择。

关于UEFI的更多信息：

- 其他有关UEFI的课程-下一页
- 参考链接：
  - 相关规范的下载网址 www.uefi.org, www.intel.com/technology/efi
  - EDK II 开放源码实现: www.tianocore.org

- Intel出版社的技术书籍： “Beyond BIOS: Implementing the Unified Extensible Firmware Interface with Intel’s Framework” www.intel.com/intelpress

EFI 专题讲座课程

课程编号	课程标题	日期/时间	教室
EFIS001 ✓	微软* Windows*平台演进与UEFI规范	周二 11:10	306A
EFIS002 ✓	片上系统（SoC）的 UEFI 开发与创新特性	周二 14:05	306A
EFIS003 ✓	UEFI 和透明计算技术	周二 15:10	306A
EFIS004 ✓	Intel® UDK2010 和Intel® BLDK： 高级嵌入式开发基础	周二 16:10	306A
SPCQ001	热点问题问答：Intel® BLDK	周二 17:00	306A
EFIS005	当前 UEFI 和Intel® UDK2010 在安全性和网络连接方面的进展	周三 11:10	306A

✓ =完毕

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, Crown Bay 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, Core, Core inside, Xeon, Xeon 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.
-

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