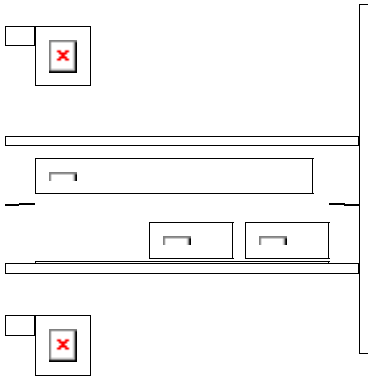
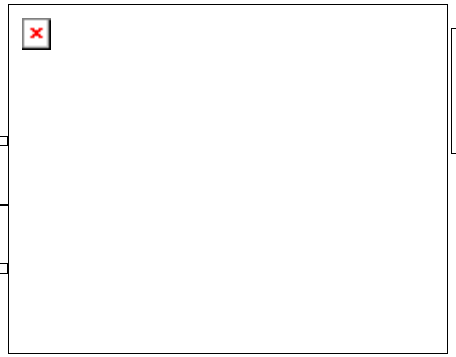
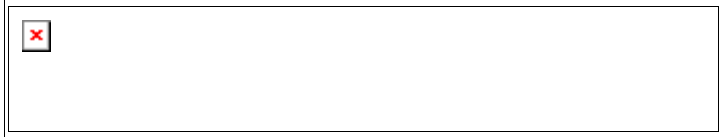






概述：基本输入输出系统(BIOS)的替代产品

从20世纪80年代起，个人计算机平台一直在迅速发展。这些进步包括性能、易用程度、存储容量和连接性的大幅度提高。但是在过去23年中电脑有一个方面一直没有发生变化，那就是BIOS(基本输入输出系统)。

用于可扩展固件接口(EFI)的英特尔® 平台创新框架(简称为“框架”)带来了为基本输入输出系统(BIOS)提供替代产品的机会，进而改善启动速度、可管理性和其它特性。

背景信息

启动固件（基本输入输出系统(BIOS)或基于框架的固件）的任务是在启动前收集硬件信息。对于可以预见的未来，构建通电未初始化的芯片和主板并不十分昂贵，因此在重启时，系统将根据这些组件恢复到通常的原始状态。

这些系统在很大程度上依靠启动固件来使系统准备好启动操作系统，为操作系统提供服务（尤其是在启动流程早期），并提供系统上的可管理性数据。

目前的问题

开始，让我们简单回顾一下在当前系统中基本输入输出系统(BIOS)的作用。基本输入输出系统(BIOS)存储在平台上一些非易失性的存储空间中，并在系统重启时开始执行。它负责系统的初始化，也就是通常所说的加电自检(POST)。

基本输入输出系统(BIOS)的POST通常用一些单片静态链接16位Real-Mode汇编语言进行编写，并转移到代码执行空间的小区域。汇编语言的结构和缺乏统一的系统服务（如先进的内存管理器）以及严格的执行空间阻止了算法和特性的开发。

除POST之外，操作系统(OS)也可以调用并为OS提供服务。在此，操作系统服务由16位软件中断提供。这些软件中断包括用于接入磁盘的Interrupt 13h、用于接入视频的Interrupt 10h和用于接入键盘的Interrupt 16h。

操作系统载入依靠这些服务的现状。这些基本输入输出系统(BIOS)服务的限制包括：扩展新服务极其困难、通过注册的参数有限、以及real-mode的限制。可扩展固件接口提供了使常规操作系统装载程序跨越不同平台体系结构（如基于IA32和英特尔® 安腾® 处理器的平台）的机遇。目前的传统OS装载系统被转到IA32 PC空间。

新技术

框架体系结构支持初始化系统并通过几个阶段为OS提

供一系列服务。每个阶段包含可用的资源、需要遵守的编码规则和结果。您可以参阅图 1 中的阶段。需要注意的是每个阶段都构建在其它阶段的基础上。

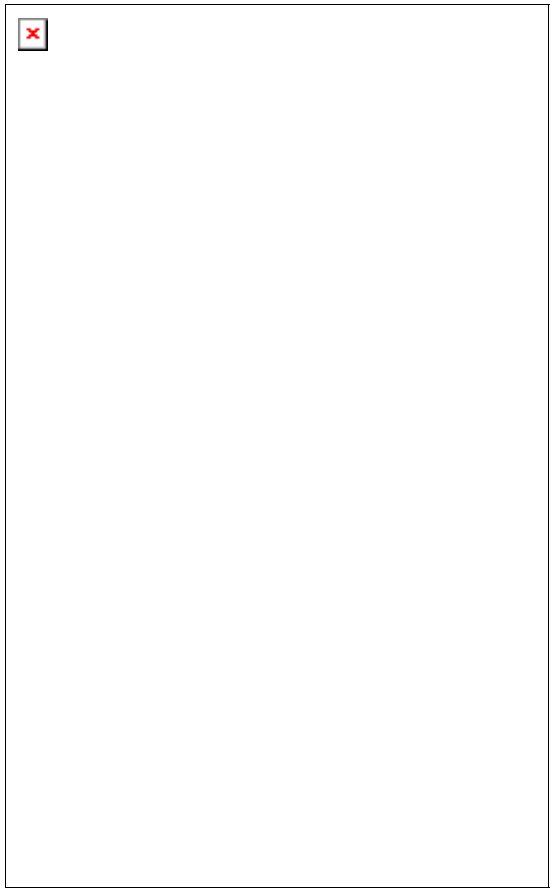
每个阶段可用的基础设施由中心框架提供，而平台的具体特性使用互连模块实施。对于EFI 前(PEI)执行阶段，模块称为PEI 模块(PEIM)。对于驱动程序执行环境(DXE)，模块可以采用DXE 或EFI 驱动程序。PEI 和DXE 的关系请参阅图2。几乎所有的基础和模块都使用portable C 代码来编写。

EFI驱动程序与OS 中的设备驱动程序有些类似。它们提供了带有扩展能力的框架体系结构，支持框架完成下列任务：

- 满足一系列平台的要求
- 结合新的计划和修理程序，以及新硬件
- 支持模块化软件体系结构

EFI 驱动程序可以在不同时间由不同的组织来开发。这里出现的问题是传统的单片BIOS 不会面对的。框架为规范EFI 驱动程序执行、抽取EFI 驱动程序接口和管理共享资源定义了强大的解决方案。在使用前，框架和EFI 驱动程序可以随意进行加密验证，以确保从加电到OS 启动及以

后都存在一个信任链。



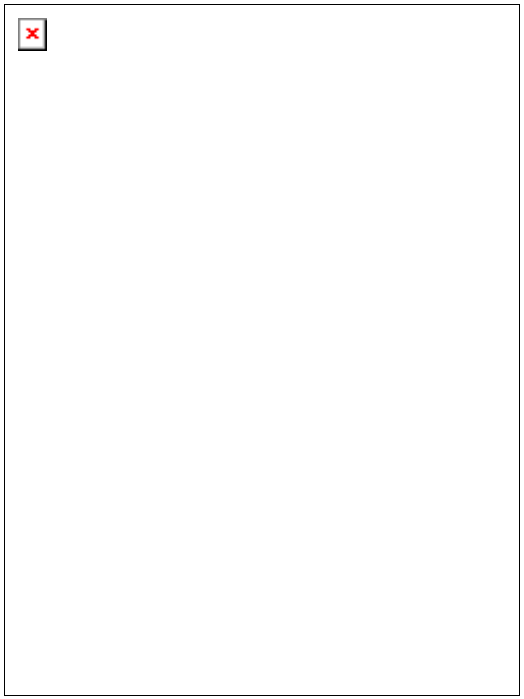
PEIM 和驱动程序可以作为单独构建的二进制模块进行部署。模块收集在一个存储区域中，也就是固件库。固件库可用于描述平台非易失性存储，以区别于其它技术。

模块到系统的接口以及模块之间的接口采用随时可用的接口，名为全球唯一标识符(GUID)。GUID 是一个 128 位的值，可以确保数字的唯一性。这种唯一性可以支持创建可扩展服务，而不会限制或造成标准和平台具体服务的冲突。

EFI“根据接口进行设计”的属性和框架可以减弱软件抽取特殊微架构和平台拓扑结构的程度。同样，框架也可以移植到IA32台式机、服务器以及内嵌式和移动系统。此外，框架也能部署在英特尔® 安腾® 架构服务器，以及基于英特尔® XScale™ 技术的平台上。值得注意的是，框架组件经过简单的交叉编译，所开发和/或再利用的模块的不同补充程序可以适应基于英特尔XScale技术的平台，一般不会阻碍部署的进行。

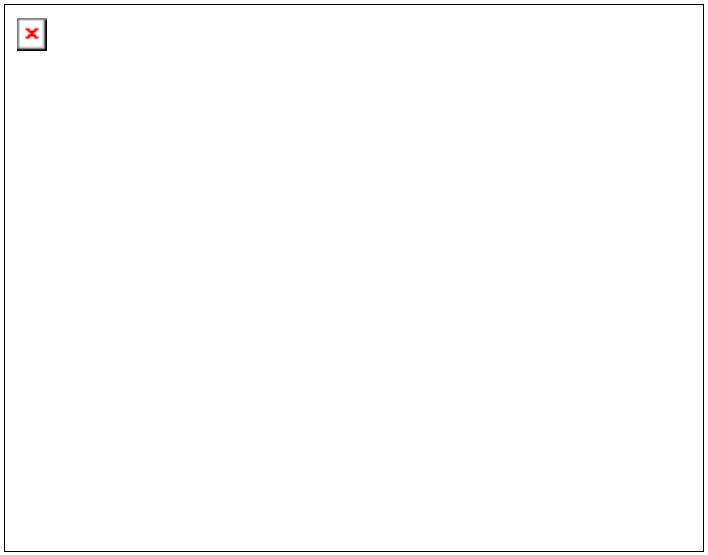
PEI和DXE阶段可以提供平台初始化向量，如内存初始化向量、I/O总线资源管理、以及在传统基本输入输出系统(BIOS)POST阶段出现的I/O设备发现。二进制模块和动态服务发现可以支持组件再利用和平台特性区分，而且无需重新链接所有代码，就像单片基本输入输出系统(BIOS)一样。

除了类似于POST的平台初始化之外，框架还可以提供OS接口。DXE阶段在其发展早期生成了一系列EFI接口。这样就可以支持空间紧张的EFI兼容接口设置部署。此外，框架同时通过一系列驱动程序为传统OS接口提供支持。这一双OS接口支持请参阅图3。



范例系统

框架可用于支持平台。下面的图4显示了类似于现有电脑平台的范例系统。主要组件包括芯片组件（蓝色）、内存技术（绿色）、I/O总线（紫色）和CPU技术（橙色）。对于使用框架的平台部署，由PEIM负责基础平台结构的初始化，包括但不限于主内存初始化和基础CPU和芯片组状态。



系统初始化的PEI阶段由PEI基础调用一系列PEIM来完成。这些PEIM包括模块北桥初始化PEIM、内存技术初始化PEIM、平台PEIM和CPU PEIM等。以CPU PEIM为例，这种隔离可以支持其在采用不同设计和芯片组的更广泛的平台上进行再利用。

一旦提供了基础平台状态，DXE执行阶段立即开始。平台初始化通常发生在DXE阶段。这里有用于PCI总线资源分配的驱动程序，与抽取容错的闪存编写接入、操控台接入（视频、USB键盘）等等的驱动程序不同。在DXE中还包括对传统OS和EFI OS启动的支持。

和PEI一样，平台的不同变化可以通过更换DXE中的一系列驱动程序来支持。不同的闪存组件或视频设备只需要各自安装一个驱动程序更新即可。此外，具有高可用性的服务器与固定配置的内嵌系统可能只是一个描述启动政策的驱动程序有所不同。

总结

用于可扩展固件接口的英特尔平台创新框架是EFI的全新产品增强型版本。它是基本输入输出系统(BIOS)的替

代产品，可以提高启动速度、加强可管理性和其它特性。框架是一系列强大的体系结构接口，部署在C中，提供了通过模块化组件构建平台固件的方式。它经过专门设计，可以支持基本输入输出系统(BIOS)行业和英特尔客户加速创新、区分和平台设计的进步。

反馈

请把您对本文的意见告诉我们。

更多信息

了解关于框架的更多信息。

了解关于可扩展固件接口的更多信息。

作者简介

Vincent Zimmer已经在英特尔工作了7年，是企业平台小组(EPG)的主任工程师。他拥有超过12年的内嵌式软件开发经验，有100多项正在申请或者已经发布的美国专利。Zimmer获得了康奈尔大学的B.S.E.E.和西雅图华盛顿大学的M.S.C.S学位。