Avanços do firmware de plataformas, para além da BIOS, e em todos os circuitos Intel®

Por Vincent Zimmer

Visão geral: Uma alternativa para o BIOS

Ocorreu uma evolução rápida da plataforma do computador pessoal a partir dos anos oitenta. Esses avanços abrangeram aumentos significativos no desempenho, na facilidade de uso, capacidade de armazenamento e conectividade. Mas existe um componente do PC que não mudou nos últimos 23 anos, ou seja, o BIOS (Basic Input/Output System).

A Intel® Platform Innovation Framework para EFI (Extensible Firmware Interface — citado como "a Estrutura") é uma oportunidade de fornecer uma alternativa para o BIOS que permita uma inicialização mais veloz, capacidade de gerenciamento e outros recursos.

Algumas considerações

A tarefa do firmware de boot (seja o BIOS ou um firmware baseado na Estrutura) é fazer uma coleção do hardware antes do boot parecer um sistema completo, após o boot. É possível prever que será menos dispendioso, mais adiante, construir chips e placas que funcionem sem inicialização de modo que, quando reiniciados, os sistemas baseados nesses componentes estejam em um estado geralmente primitivo.

Esses sistemas dependem muito do firmware de boot para prepará-los para inicializar o sistema operacional, fornecer serviços ao sistema operacional (principalmente no início do processo de boot) e dados da capacidade de gerenciamento no sistema.

Questões atuais

Para início de conversa, examinemos a função do BIOS no sistema atual. O BIOS é guardado em um armazenamento não-volátil na plataforma e começa a funcionar ao reiniciar o sistema. O BIOS é o responsável pela inicialização do sistema. Isso é citado geralmente como POST (power-on self test).

O POST do BIOS é escrito, em geral, em uma linguagem de montagem em modo real, monolítica, de 16 bits vinculados estaticamente, e está relegado a uma pequena área do espaço do código de execução. A construção da linguagem de montagem e a falta de serviços de sistema consistentes, como um gerenciador da memória do modem, aliado à restrição do espaço de execução, impede o desenvolvimento de algoritmos e recursos.

Além do BIOS, existe a chamada ao sistema operacional (SO) e a possibilidade de fornecer serviços para o SO. Neste caso, os serviços do sistema operacional são fornecidos por interrupções de software de 16 bits. Essas interrupções são a 13h para acesso ao disco, a 10h para acesso ao vídeo e a 16h para acesso ao teclado.

Os carregamentos do sistema operacional dependem da existência desses serviços. As limitações desses serviços do BIOS são a dificuldade em expandir novos serviços, a passagem limitada de parâmetros através dos registradores e as restrições do modo real. A EFI (Extensible Firmware Interface) é uma oportunidade de se ter um carregador comum do sistema operacional para arquiteturas de plataformas diferentes, como a IA32 e as plataformas baseadas no processador Itanium® da Intel®. O carregador do sistema operacional existente hoje em dia está relegado ao mundo do PC IA32.

Nova tecnologia

A arquitetura da Estrutura (Framework) tem suporte para os requisitos de inicializar um sistema e fornecer serviços para o SO por meio de uma série de fases. Cada fase é caracterizada pelos recursos disponíveis, as regras que o código na fase deve obedecer, e os resultados da fase. É possível ver as fases na **Figura 1**. Convém observar que cada fase depende da outra.

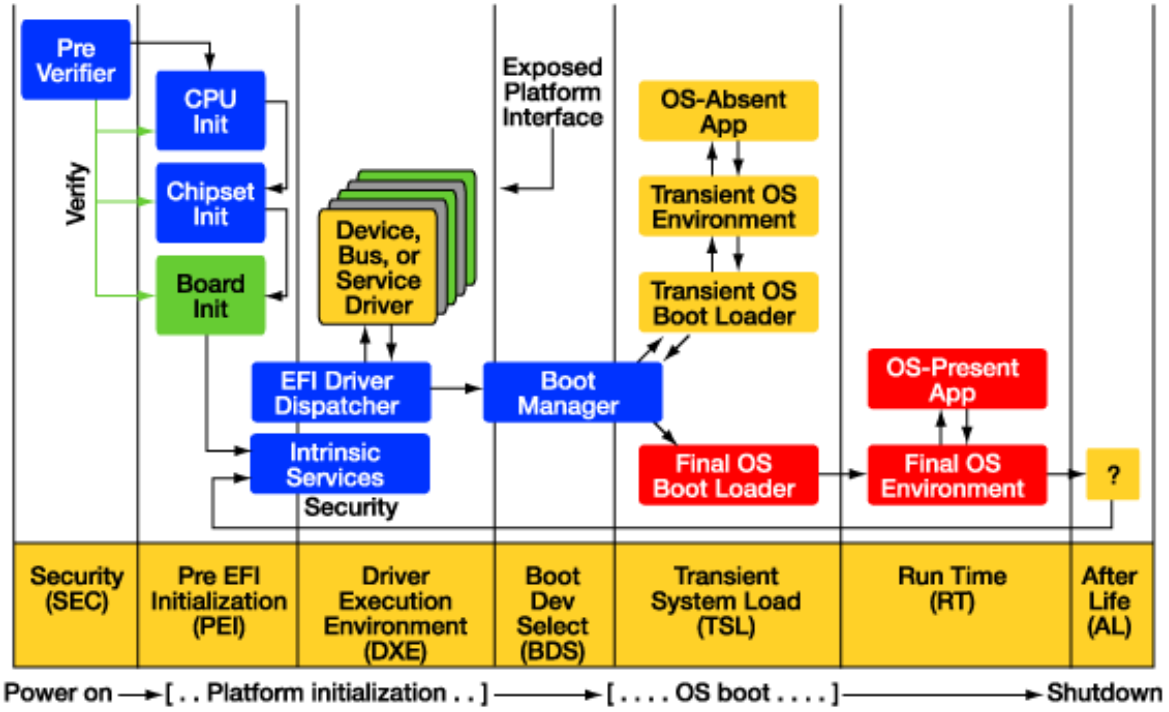

Figura 1. Fluxo do firmware.

A infra-estrutura disponível em cada fase é fornecida pela estrutura central, embora os recursos específicos da plataforma sejam implementados por meio dos módulos de intercomunicação. Para a fase Pré-EFI (PEI) de execução, os módulos são conhecidos como módulos PEI (PEIMs). Para o ambiente de execução de drivers (DXE), os módulos são alternativamente os drivers DXE ou EFI. O relacionamento entre o PEI e o DXE pode ser visto na **Figura 2**. Praticamente toda a base e os módulos são escritos em código C portável.

Os drivers EFI são parecidos com os drivers de dispositivos nos SOs. Eles propiciam à arquitetura da Estrutura (Framework) sua extensibilidade e permitem o seguinte:

- Atender às exigências de diversas plataformas.
- Incorporar novas iniciativas e consertos, além de novo hardware.
- Suportar arquitetura de software modular

Os drivers EFI podem ser desenvolvidos em diferentes ocasiões e por organizações distintas. Isso traz problemas que os BIOS's tradicionais monolíticos não enfrentavam. A Estrutura define soluções poderosas para seqüenciar a execução dos drivers EFI, abstraindo as interfaces desses drivers e gerenciando recursos compartilhados. Como opção, a Estrutura e os drivers EFI podem ser validados de modo criptográfico antes de serem usados, para garantir um seqüenciamento seguro desde quando o sistema é ligado até os boots do SO e mais além.

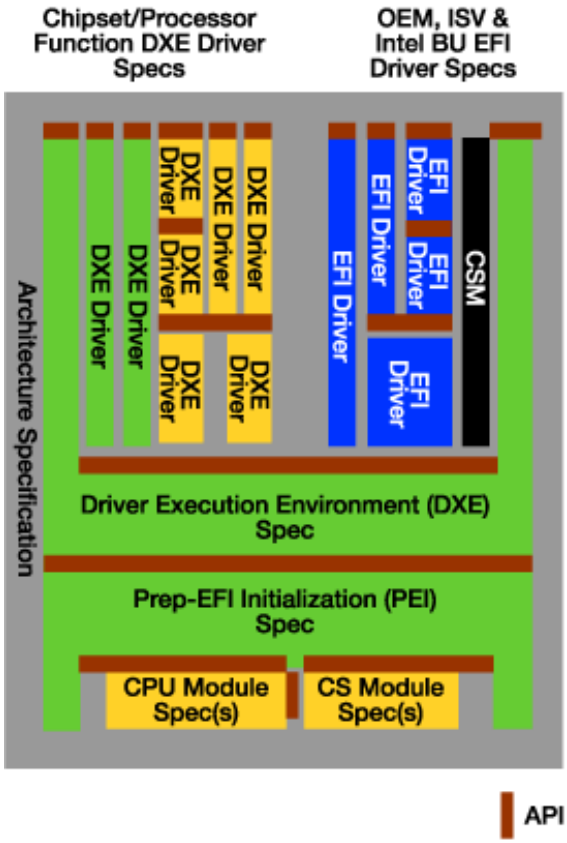

Figura 2. Módulos binários da Estrutura.

Os PEIMs e os drivers podem ser desenvolvidos como módulos binários construídos separadamente. Os módulos são reunidos em uma abstração de armazenamento conhecida como volume do firmware. O volume do firmware pode ser usado para descrever o armazenamento não-volátil da plataforma, entre outras tecnologias.

Os módulos fazem interface com o sistema e entre si via interfaces chamáveis, denominadas GUIDs (Globally Unique Identifiers — Identificadores Globalmente Exclusivos). O GUID é um valor de 128 bits garantido como estaticamente exclusivo. Essa exclusividade permite cirar serviços extensíveis sem limitações ou colisões entre os serviços padrão e os específicos das plataformas.

A natureza de projeto por interface da EFI e a Estrutura desassocia as abstrações de software da microarquitetura específica e topologias de plataforma. Como tal, a Estrutura tem sido portada para os sistemas desktop IA32, de servidores, incorporados e portáteis. Além disso, a Estrutura foi desenvolvida em servidores baseados no processador Itanium até as plataformas baseadas na tecnologia Intel XScale®. Convém observar que os componentes da Estrutura foram simplesmente submetidos a uma compilação cruzada e um diferente complemento de módulos foi desenvolvido e/ou reutilizado para acomodar as plataformas baseadas na tecnologia Intel XScale, de modo a não impedir o desenvolvimento.

As fases PEI e DXE providenciam a inicialização da plataforma, como a inicialização da memória, gerenciamento de recursos do barramento de E/S e detecção dos dispositivos de E/S, que ocorria durante a fase POST dos BIOS existente. Os módulos binários e a detecção de serviços dinâmicos permitem reutilizar os componentes e diferenciar os recursos da plataforma sem precisar vincular novamente todo o código, como acontece com um BIOS monolítico.

Além da inicialização da plataforma ao estilo POST, a Estrutura se encarrega da interface do SO. A fase DXE gera um grupo de interfaces EFI no início de sua evolução. Isso permite a implementação de um conjunto de interfaces compatíveis com a EFI, levando em consideração o espaço. Adicionalmente, a Estrutura dispõe de suporte para as interfaces do SO existente através de um conjunto de drivers. O suporte para a interface do SO-duplo pode ser visto na **Figura 3**.

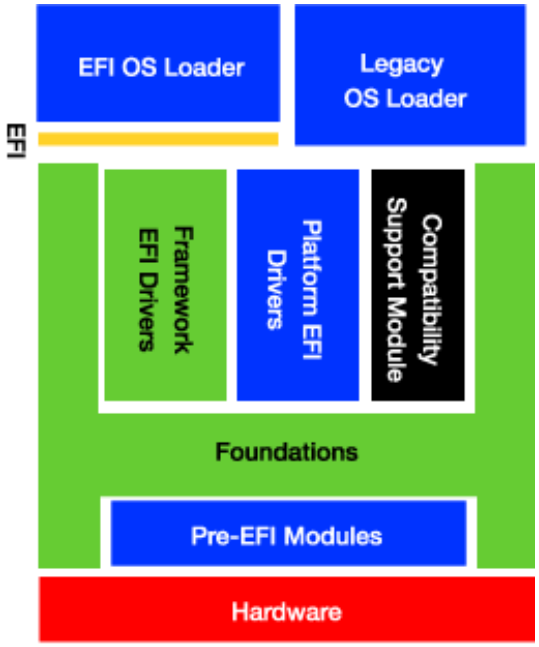

Figura 3. Camadas de software.

Exemplo de sistema

A Estrutura pode ser usada para dar suporte a uma plataforma. A **Figura 4** abaixo mostra um exemplo de sistema semelhante à plataforma do PC atual. Os componentes destacados são os de silício (azul), a tecnologia de memória (verde), barramentos de E/S (roxo) e a tecnologia de CPU (laranja). Para o desenvolvimento de uma plataforma com a Estrutura (Framework), existem PEIMs responsáveis pela inicialização da construção da plataforma básica, incluindo (mas não limitado a) a inicialização da memória principal e o estado da CPU básico e dos chipsets.

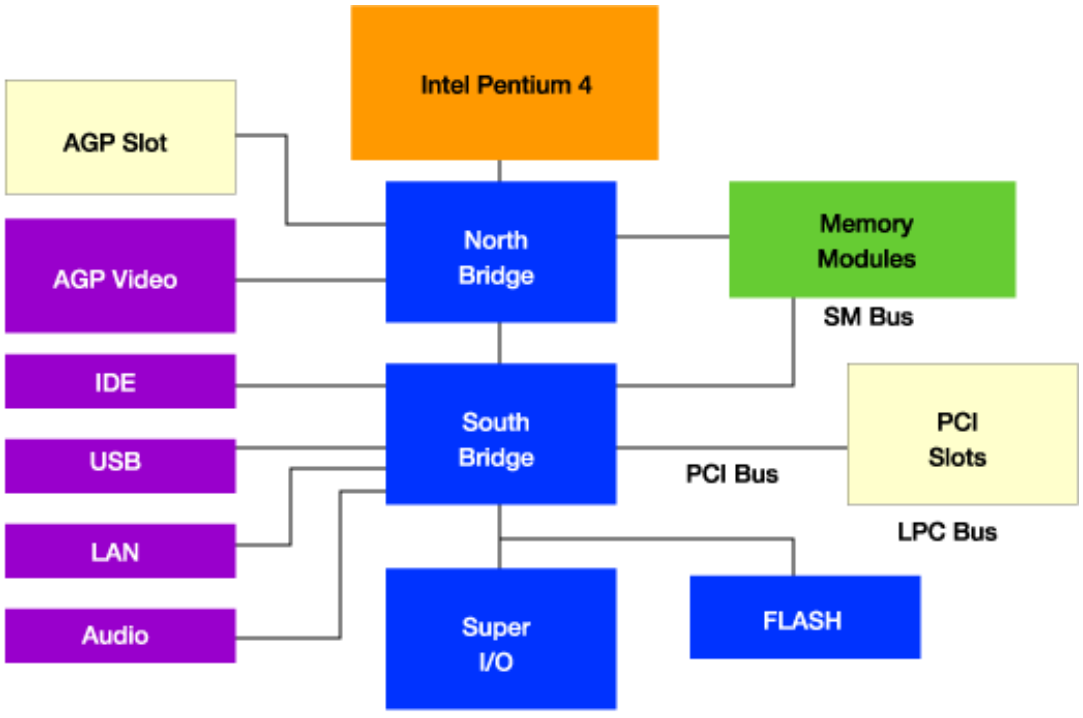

Figura 4. Diagrama de blocos do sistema.

A fase PEI da inicialização do sistema prossegue quando a base PEI chama um conjunto de PEIMs. Esses PEIMs abrangem módulos como o PEIM de inicialização de North Bridge, o de iniciação da tecnologia de memória, o da plataforma e o PEIM da CPU. Essa separação permite ter um PEIM da CPU, por exemplo, que pode ser reutilizado em uma grande classe de

plataformas com diferentes projetos e chipsets.

Assim que o estado da plataforma básica for providenciado, começa a fase DXE de execução. A maior parte da inicialização da plataforma ocorre durante a fase DXE. Aqui, existiria um driver para a alocação de recursos do barramento PCI, outro driver para abstrair o acesso para gravação com tolerância a falhas à memória flash, acesso ao console (vídeo, teclado USB) etc. É também na fase DXE que é fornecido o suporte para o SO existente e para a inicialização do SO da EFI.

Examente como no caso da PEI, diferentes permutações da plataforma podem ser suportadas na DXE, com a substituição de alguns conjuntos de drivers. Um componente flash ou dispositivo de vídeo diferente exigiriam apenas uma simples atualização de driver, respectivamente, em cada caso. Além disso, a única diferença entre um servidor de alta disponibilidade e um sistema incorporado com configuração fixa pode ser tão-somente um driver que descreve o procedimento de boot.

Resumo

A Intel Platform Innovation Framework para EFI (Extensible Firmware Interface) é uma nova implementação mais poderosa da EFI, que oferece uma alternativa para o BIOS, permitindo uma inicialização mais rápida, capacidade de gerenciamento e recursos adicionais. A Estrutura é um conjunto de interfaces arquitetônicas robustas, implementadas em linguagem C, que permite construir o firmware da plataforma por meio de componentes modulares. Essa Estrutura foi elaborada para permitir que o setor de BIOS e os clientes da Intel acelerassem a evolução de projetos de plataformas diferenciados e inovadores.