Avances de firmware de plataformas para más allá del BIOS y en todos los circuitos Intel®

Por Vincent Zimmer

Generalidades: Una alternativa del BIOS

Ha habido una rápida evolución de la plataforma de computadoras personales desde los años ochenta. Estos avances han incluido incrementos de magnitud en cuanto a rendimiento, facilidad de uso, capacidad de almacenamiento y conectividad. Pero hay un elemento en la PC que no ha cambiado en los últimos 23 años, a saber, el BIOS (sistema básico de entradas/ salidas).

La Estructura de innovación de la plataforma de Intel® para la Interfaz de firmware extensible (EFI) (en adelante, "la Estructura") ofrece una oportunidad para proporcionar una alternativa al BIOS que permita un inicio más rápido, administrabilidad y características adicionales.

Algo de antecedentes

La tarea del firmware de inicio (independientemente de si el BIOS o firmware está basado en la Estructura) es hacer que un conjunto de hardware antes del inicio se vea como un sistema completo después del mismo. Para el futuro próximo, es menos costoso fabricar chips y placas que se enciendan sin inicializarse de manera que, cuando se restablezcan, los sistemas erigidos alrededor de estos componentes estén en un estado normalmente primitivo.

Estos sistemas dependen en gran parte en el firmware de inicio para preparar el sistema para iniciar el sistema operativo, proporcionar servicios al sistema operativo (particularmente en la etapa inicial del proceso de inicio) y proporcionar información de administrabilidad en el sistema.

Problemas de hoy

Para comenzar, revisemos el papel al BIOS en un sistema de hoy. El BIOS se guarda en algún almacenamiento no volátil en la plataforma y comienza a ejecutarse al reiniciar el sistema. El BIOS es responsable de la inicialización del sistema. Normalmente esto se conoce como la autoprueba de encendido (POST).

La POST del BIOS normalmente se escribe en algún lenguaje ensamblador de modo real, monolítico, que está vinculado estáticamente a los 16 bits y se relega a una pequeña región de espacio de código para su ejecución. La construcción del lenguaje ensamblador y la falta de servicios de sistema consecuentes, como un administrador moderno de memoria, aunados al espacio restringido de ejecución, impiden el desarrollo de algoritmos y funciones.

Más allá de la POST, está la invocación del sistema operativo (SO) y la capacidad de ofrecer servicios al mismo. Aquí, los servicios del sistema operativo son proporcionados por interrupciones de software de 16 bits. Estas interrupciones de software incluyen la interrupción 13h para acceder al disco, la interrupción 10h para acceder al vídeo y la interrupción 16h para acceder al teclado.

Las cargas del sistema operativo se basan en la existencia de estos servicios. Las limitaciones de estos servicios del BIOS incluyen la dificultad para extender nuevos servicios, el paso limitado de parámetros a través de los registros y las restricciones del modo real. La Interfaz de firmware extensible ofrece una oportunidad para tener un cargador común de sistema operativo para todas las distintas arquitecturas de plataformas, como las plataformas basadas en IA32 y en el procesador Intel® Itanium®. El cargador heredado de sistemas operativos de hoy está relegado al mundo de las PC de IA32.

Nueva tecnología

La arquitectura de la Estructura es compatible con estos requerimientos de inicialización de un sistema y de generación de servicios para el sistema operativo a través de una serie de fases. Cada fase se caracteriza por los recursos que están disponible para ella, las reglas a las que se debe sujetar el código en la fase y los resultados de ésta. Puede ver las fases en la **figura 1**. Se debe notar que cada fase se erige encima de la otra.

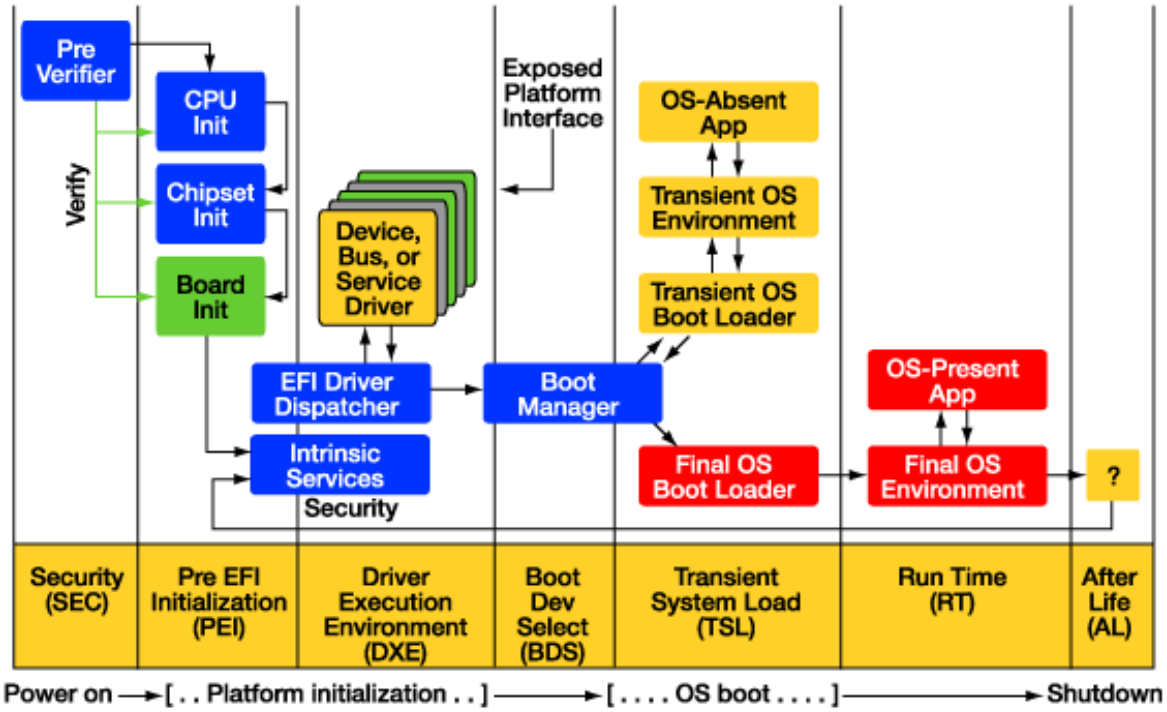

Figura 1. Flujo del firmware.

La infraestructura disponible en cada fase la proporciona la estructura central, en tanto que las funciones específicas de una plataforma se implementan mediante módulos de intercomunicación. Para la fase de ejecución previa a la EFI (PEI), los módulos se conocen como módulos PEI (PEIM). Para el entorno de ejecución del controlador (DXE), los módulos son controladores DXE o EFI. La relación de la PEI y el DXE se puede ver en la **figura 2**. Casi toda la base y los módulos están escritos en código C portátil.

Los controladores EFI son de alguna manera análogos a los controladores de dispositivos en los sistemas operativos. Ellos proporcionan la arquitectura de la Estructura con su extensibilidad y le permiten realizar lo siguiente:

- Cumplir los requisitos de una variedad de plataformas
- Incorporar nuevas iniciativas y arreglos, así como nuevo hardware
- Admitir arquitectura modular de software

Los controladores EFI se pueden desarrollar en momentos distintos por parte de distintas organizaciones. Esto presenta problemas que los BIOS tradicionales y monolíticos no enfrentan. La Estructura define soluciones de gran poder para secuenciar la ejecución de controladores EFI, abstraer interfaces de controladores EFI y administrar recursos compartidos. Es posible que la Estructura y los controladores EFI opcionalmente puedan validarse de manera criptográfica antes de su utilización a fin de asegurar que exista una cadena de confianza desde el encendido hasta que el sistema operativo se inicie y aún después.

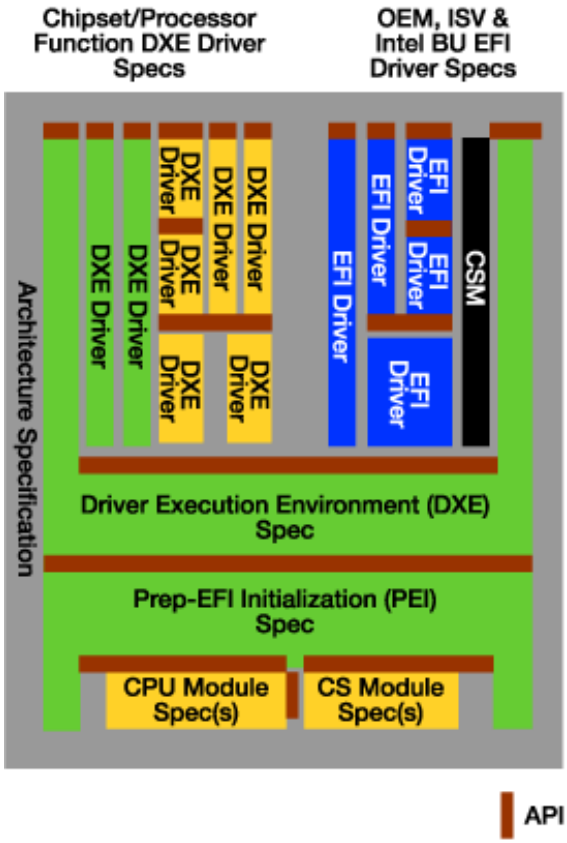

Figura 2. Módulos binarios de la Estructura.

Los módulos PEIM y los controladores se pueden instalar como módulos binarios construidos por separado. Los módulos se recopilan en una abstracción de almacenamiento conocida como un volumen de firmware. El volumen de firmware se puede utilizar para describir el almacenamiento no volátil de la plataforma, entre otras tecnologías.

Los módulos realizan una interfaz con el sistema y entre sí por medio de interfaces ejecutables que reciben su nombre de identificadores únicos globales (GUID). El GUID es un valor de 128 bits que se garantiza como estadísticamente único. Esta singularidad permite la creación de servicios extensibles sin limitación ni colisión entre los servicios estándares y específicos de una plataforma.

La naturaleza de "diseño por interfaz" de la EFI y la Estructura separan las abstracciones de software de las topologías de plataforma y la microarquitectura particular. Como tal, la Estructura se ha implementado en sistemas de escritorio, de servidor, incorporados y móviles de IA32. Asimismo, la Estructura se ha instalado en los servidores basados en el procesador Itanium abarcando las plataformas basadas en la tecnología XScale® de Intel. Se debe hacer notar que los componentes de la Estructura simplemente fueron compilados entre sí y se desarrolló o se volvió a usar un complemento distinto de módulos a fin de incluir las plataformas basadas en la tecnología XScale de Intel, de manera que no se impidiera su implantación.

Las fases de la PEI y el DXE dan servicios a la inicialización de la plataforma, por ejemplo, la inicialización de la memoria, la administración de recursos del bus de E/S y el descubrimiento de dispositivos de E/S que se presentan durante la fase de la POST del BIOS heredado. El descubrimiento de servicios dinámico y los módulos binarios permiten volver a utilizar componentes y hacer distinción de funciones de plataformas sin tener que volver a vincular todo el código, como ocurre con un BIOS monolítico.

Además de la inicialización de plataforma similar a la POST, la Estructura da servicio a la interfaz del sistema operativo. La fase del DXE da origen a un conjunto de interfaces de EFI en la etapa temprana de su evolución. Esto permite la implementación, teniendo en cuenta el espacio, de un conjunto de interfaces que cumple con los estándares de la EFI. Además, la Estructura proporciona soporte para las interfaces del sistema operativo heredado por medio de un conjunto de controladores. Este soporte de interfaz de doble sistema operativo se puede ver en la **figura 3**.

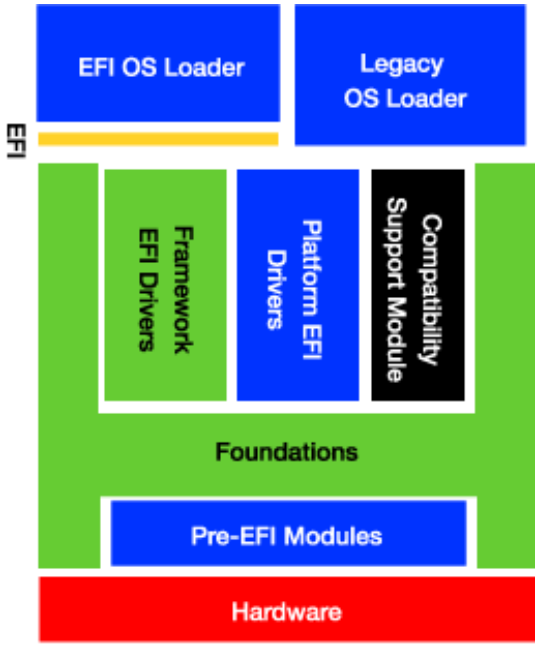

Figura 3. Tendido de capas de software.

Sistema de ejemplo

La Estructura se puede usar para sustentar una plataforma. La **figura 4** a continuación muestra un sistema de ejemplo similar a la plataforma de PC de hoy. Los componentes más notables incluyen componentes de silicio (azul), tecnología de memoria (verde), buses de E/S (morado) y tecnología de CPU (naranja). Para la instalación de una plataforma con la Estructura, hay módulos PEIM que son responsables de la inicialización del tejido de plataforma básico, incluyendo, entre otros, la inicialización de la memoria principal y el estado básico de la CPU y el chipset.

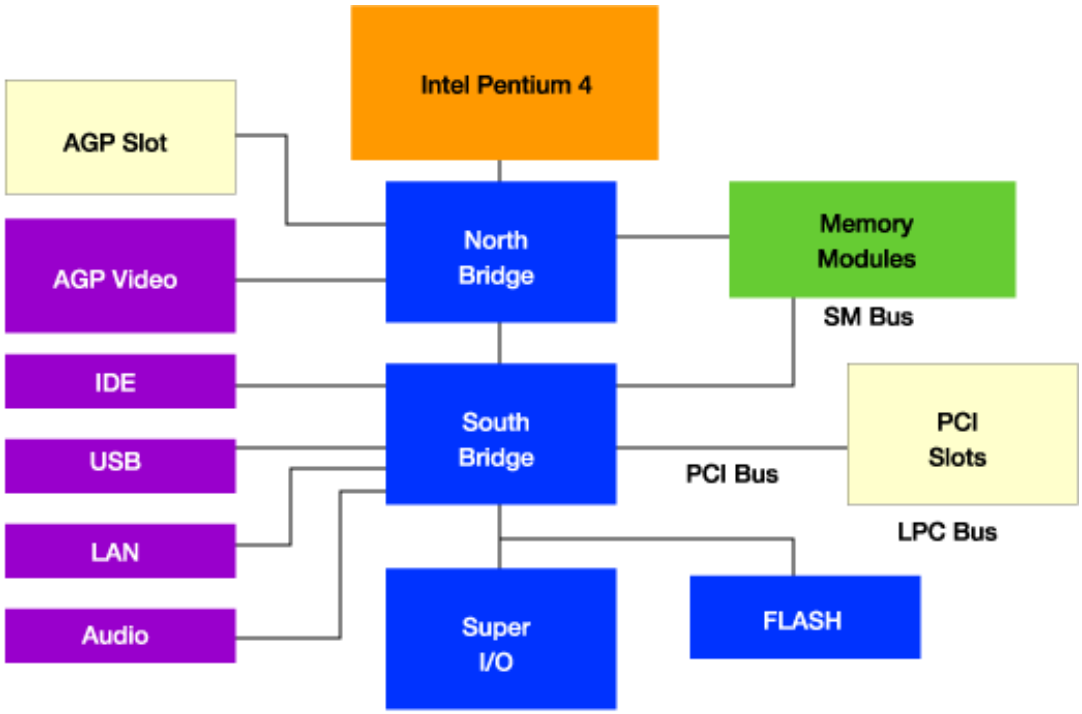

Figura 4. Diagrama de bloques del sistema.

La fase de la PEI de inicialización del sistema procede haciendo que el cimiento de la PEI invoque una recopilación de módulos PEIM. Estos PEIM incluyen módulos como el PEIM de inicialización de North Bridge, el PEIM de inicio de la tecnología de memoria, el PEIM de la plataforma y un PEIM de la CPU. Esta segregación permite tener un PEIM de la CPU, por ejemplo, que se pueda volver a usar entre una amplia clase de plataformas con distintos diseños y chipsets.

Una vez que el estado básico de plataforma se haya proporcionado, comenzará la fase de ejecución del DXE. La mayor parte de la inicialización de la plataforma ocurre durante la fase del DXE. Aquí, habrá un controlador de asignación de recursos de bus PCI, un controlador distinto para el acceso de lectura abstracto con tolerancia a fallas en la memoria flash, un acceso de consola (vídeo, teclado USB), etc. En el DXE es también donde se proporciona el soporte para los inicios de sistemas operativos EFI y los de sistemas operativos heredados.

Al igual que en la PEI, en el DXE se admiten distintas permutaciones de la plataforma mediante el reemplazo de algunos conjuntos de controladores. Un dispositivo de vídeo o un componente de memoria flash distinto supondrá únicamente una sola actualización de controlador, respectivamente, en cada caso. Asimismo, es posible que un servidor de alta disponibilidad en comparación con un sistema incorporado de configuración fija sólo difieran en un solo controlador que describa la política de inicio.

Resumen

La Estructura de innovación de plataforma de Intel para la Interfaz de firmware extensible es una nueva implementación de fortaleza de producto de la EFI. Ofrece una alternativa para el BIOS que habilitará un inicio más rápido, administrabilidad y funciones adicionales. La Estructura es un conjunto de interfaces de arquitectura robustas, implementadas en C, que ofrece una manera de construir firmware de plataformas a través de componentes modulares. Ha sido diseñada para hacer posible que la industria del BIOS y los clientes de Intel aceleren la evolución de diseños de plataforma innovadores y diferenciados.