Evaluating UEFI using Commercially Available Platforms and Solutions

An UEFI Industry Communications Working Group (ICWG) Paper

Version 0.31
February 16, 2010

Foreword:

In recent trade shows, training events, and the overall UEFI promotional events, there has been a reoccurring question by interested technologists and developers assigned to explore and evaluate UEFI technology:

How can I experiment with the UEFI interfaces with currently available platform technology?

This question has several answers, and will require some background data to fully understand the available resources for development, evaluation, and experimentation with UEFI.

UEFI is an interface standard, and while the interface is consistent and well defined, it is possible to have several implementations which conform to the standard. This is important, as it allows for flexibility in the industry, while still maintaining a known standard of conformance.

Bearing this in mind, there are four classes of PC platforms in the industry that need to be discussed as there are methods for performing UEFI experimentation on all of these platform classes:

Definition of Terms:

Class Zero (or non-UEFI Platforms, also referred to as Traditional BIOS platforms): This set of platforms is based upon the original BIOS technology of the 1980's. They are not inherently UEFI aware, but rather represent the pre-UEFI state of technology. They are mentioned, as there are still several methods of performing UEFI experimentation using a traditional BIOS platform by the use of UEFI simulation over the traditional BIOS, or the Operating System(OS) (for limited experimentation – see below).

This class is defined as those platforms that have NO UEFI awareness in their design, and are based upon the original PC BIOS architecture.

Class One: In 2003 some PC class platforms began to ship with EFI (the pre-cursor to UEFI) technology integrated as the firmware boot solution. As an introductory technology, the EFI interface was not published beyond the pre-boot environment, and a special software driver (designated the CSM – Compatibility Support Module) was used to provide the runtime and operating system interfaces expected of the traditional BIOS solution. To the average user, this change in firmware design was completely transparent, and for all intents and purposes the inclusion of EFI in the platform had no impact on the end user.

EFI/UEFI does provide advantages to the system developers and manufacturers that are not obvious to the users. The modular design of EFI/UEFI allowed developers to reuse established code over multiple platforms and products, both reducing development time

and increasing code reliability. EFI/UEFI also provides a robust pre-execution environment for manufacturing organizations to qualify and validate platform system before customer ship. So while the customer may not have seen any appreciable change between a EFI/UEFI boot solution with Compatibility Support and the traditional PC BIOS, those changes were being exploited.

While these platforms are UEFI enabled, individuals wishing to experiment with the UEFI interfaces on these platforms would experience difficulty, as the design prevents the publication the UEFI interfaces to the user.

Class Two: Defined as a computer system which provides the ability to perform a boot strap (or application execution) through the use of the UEFI defined boot process using an UEFI boot loader applications (through UEFI interfaces). However, Class Two systems also support the Tradition BIOS INT 19h boot process (load a boot image from a specific device location to a hard coded memory location and transferring execution to that loader).

This allows the system to support both boot standards, as well as take advantage of the added pre-boot features of UEFI (Shell application, UEFI applications and utilities, UEFI feature extensions that are not possible in the traditional BIOS environment).

At this time, system vendors are beginning to include an option to publish and execute in an UEFI environment as well as a CSM environment (Class Two systems). These systems will allow a user access to the UEFI interfaces that were inherently part of the pre-boot system design as part of the native BIOS code, or allow the user to perform a traditional BIOS boot to a non-UEFI aware operating environment.

Class Three: Defined as a system which provides the ability to perform a boot strap (or application execution) through the use of the UEFI defined boot process using an UEFI boot loader applications (through UEFI interfaces), but without the CSM option as an integral part of the system BIOS support. In reality, the CSM option could be provided in a Class Three system as an after market add-on, but Class three is defined as a system with no integrated facilities for non-UEFI booting.

Simulation Environments:

Currently, there are two simulation environments available for developers to experiment with the UEFI interfaces on systems not publishing those interfaces to the users (Class Zero and One). Both of these environments are available on the UEFI Open Source Community Website (URL: www.Tianocore.org). They are both available through the EDK and EDK2 projects on this website, and documentation and manuals are available on the website as well (along with some very helpful discussion groups, whose participants have demonstrated great patience and zeal in helping new comers over technical issues).

NT32: This simulation environment allows the user to operate an UEFI compatible simulation environment while running the Microsoft Windows OS. This environment provides the user a good look at the interfaces, protocols and overall inter-operability of UEFI, as well as the ability to develop some applications for UEFI, while running a standard operating system. The drawback to NT32 is that the Operating System is very protective of the hardware interfaces of the platform upon which it executes so UEFI drivers and applications attempting to directly interact with the hardware (which includes all hardware drivers), will generate an OS exception and terminate the simulation environment.

However for the purposes of early driver design, the development of applications, and general experimentation with UEFI, NT32 represents a useful enabling tool.

DUET: This simulation environment avoids the Operating system limitation of NT32, but generating bootable (under a traditional BIOS Boot process) device (disk, CD, USB thumb drive) and allowing the platform to "boot" into an UEFI environment as a extension of the standard OS boot process. Since the OS is not loaded with DUET, the hardware is not under the OS protection, and the developer may interact with the hardware freely.

DUET is a very useful tool, and has been used by several hardware developers as the initial development and test environment for UEFI drivers for their products.

Interaction Matrix:

Platform Class	NT32	Duet	Native UEFI interfaces
Class Zero	Yes	Yes	No
Class One	Yes	Yes	No
Class Two	Yes (In OS – But this is redundant)	Yes (In CSM Mode – But this is redundant)	Yes
Class Three	Yes (But this is redundant)	No (Not necessary)	Yes

Beyond Simulation:

In the end, many developers are not interested in simulations, but in real platforms, with UEFI pre-boot, which also publishes those interfaces so that the user may experiment with them directly and natively.

Below is a list of Class Two and Class Three products that are now commercially available. This list is not exhaustive, but was compiled from data provided by members

of the UEFI and through publically available websites. It will be updated as more such systems become known to the UEFI Forum.

The UEFI's Industry Communications Working Group (ICWG) invites vendors to inform us of additional platforms to add to this list as they become commercially available. Please contact Michael Krau (The Chair of the ICWG) at Michael.p.krau@intel.com to provide updates to this list.

Dell:

Dell PowerEdge T610 Tower Server
http://www.dell.com/content/products/productdetails.aspx/server-poweredge-t610

Dell PowerEdge T610 Rack Server
http://www.dell.com/content/products/productdetails.aspx/server-poweredge-r610

Dell PowerEdge R710 Rack Server
http://www.dell.com/content/products/productdetails.aspx/server-poweredge-r710

Dell PowerEdge M710 Blade Server
http://www.dell.com/content/products/productdetails.aspx/server-poweredge-m710

Dell PowerEdge M610 Blade Server
http://www.dell.com/content/products/productdetails.aspx/server-poweredge-m610

Dell Unified Sever Configurator
http://www.dell.com/downloads/global/solutions/unified_server_overview.pdf

HP:

HP EliteBook Mobile Workstation, Notebook PC and Tablet PCs (e.g., 8530p, 8530w, 8730w, 6930p, 2530p, 2730p, etc)
http://www.hp.com/sbso/busproducts_notebooks.html

HP Compaq NoteBook PCs (e.g., 6735s, 6535s, 6735b, 6535b, 6730s, 6830s, 6530b, 6730b, 2230s, etc.)
http://www.hp.com/sbso/busproducts_notebooks.html

A HP white paper "Installing UEFi-based Microsoft Windows Vista SP1 (x64) on HP EliteBook and Compaq Notebook PCs":
http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01717787/c01717787.pdf?jumpid=reg_R1002_USEN

(Class 3) HP Integrity Servers and Server Blades
http://h71028.www7.hp.com/enterprise/cache/80518-0-0-0-121.html

IBM:

System x3550 M2
http://www-03.ibm.com/systems/x/hardware/rack/x3550m2/index.html

System x3650 M2
http://www-03.ibm.com/systems/x/hardware/rack/x3650m2/index.html

Blade Center HS22
http://www-03.ibm.com/systems/bladecenter/hardware/servers/hs22/index.html

iDataPlex dx360 M2
http://www-03.ibm.com/systems/x/hardware/idataplex/dx360M2/index.html

IBM x3450 server
http://www-304.ibm.com/shop/americas/webapp/wcs/stores/servlet/default/ProductDisplay?productId=4611686018425779005&storeId=1&langId=-1&categoryId=4611686018425232005&dualCurrId=73&catalogId=-840

(Class 3) IBM eServer xSeries 455
https://www-304.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-58415&brandind=5000008

Intel:

Intel motherboards DP55WB, DP55WG, DP55Kg, DP55SB
http://www.intel.com/products/desktop/motherboards/dp55Wb/dp55wb-overview.htm
http://www.intel.com/products/desktop/motherboards/dp55Wg/dp55wg-overview.htm
http://www.intel.com/products/desktop/motherboards/dp55kg/dp55kg-overview.htm
http://www.intel.com/products/desktop/motherboards/dp55sb/dp55sb-overview.htm

DP43TF, DG43NB, DG41TY, DQ45EK, DQ45CB, DG45ID, DG45FC, DG41RQ, DG33BU, DG33FB,DG33TL, DP35DP series, with a BIOS update from Intel.com (version 0497 – October 7, 2008 or later).
http://www.intel.com/products/desktop/motherboards/DP43TF/DP43TF-overview.htm
http://www.intel.com/products/desktop/motherboards/DG43NB/DG43NB-overview.htm
http://www.intel.com/products/desktop/motherboards/DG41TY/DG41TY-overview.htm
http://www.intel.com/products/desktop/motherboards/DQ45EK/DQ45EK-overview.htm
http://www.intel.com/products/desktop/motherboards/DQ45CB/DQ45CB-overview.htm
http://www.intel.com/products/desktop/motherboards/DG45ID/DG45ID-overview.htm
http://www.intel.com/products/desktop/motherboards/DG45FC/DG45FC-overview.htm
http://www.intel.com/products/desktop/motherboards/DG41RQ/DG41RQ-overview.htm
http://www.intel.com/products/desktop/motherboards/DG33BU/DG33BU-overview.htm
http://www.intel.com/products/desktop/motherboards/DG33BU/DG33BU-overview.htm
http://www3.intel.com/cd/channel/reseller/asmo-na/eng/products/desktop/bdb/dg33tl/feature/index.htm

http://www.intel.com/products/desktop/motherboards/DP35DP/DP35DP-overview.htm

MSI:

MSI Motherboards (P45D3 Platinum, Efinity (only available in Taiwan), etc.) (Click BIOS)
http://global.msi.com.tw/html/popup/MB/uefi/applied_model.html

MSI Wind (Netbook)
http://www.msicomputer.com/NB/index.asp

Panasonic:

(Class 2) Panasonic Toughbook CF-U1 (Atom UMPC)
http://www.panasonic.com/business/toughbook/ultramobile-rugged-computers.asp