Simplifying Firmware Development with Intel® Unified Binary Management Suite

Mark Doran – Intel Fellow, Intel Corporation
Brian Richardson – Senior Technical Marketing Engineer, Intel Corporation
Agenda

- Firmware Challenges
- Intel® Unified Binary Management Suite (Intel® UBMS)
- Use Cases for Intel UBMS
- Intel UBMS Ecosystem
- Summary / Call to Action
Agenda

• Firmware Challenges
  • Intel® Unified Binary Management Suite (Intel® UBMS)
  • Use Cases for Intel UBMS
  • Intel UBMS Ecosystem
• Summary / Call to Action
Firmware Challenges

Intel® Architecture (IA) has an established firmware ecosystem ...

• Third-party enabling from Independent BIOS Vendors (IBV)
• Open source projects such as tianocore.org & coreboot.org
• Intel® Firmware Support Package (Intel® FSP) for low-level initialization

However, there are still barriers for some IA platform designers ...

• No path for customers without IA firmware experience
• Must remove learning curve for creating derivative designs
• Address low-cost markets with minimal firmware requirements
Enabling Firmware for Derivative Designs

Look at a common reference design for Intel powered tablets ...

• Reference design includes UEFI firmware that boots to the OS

OEM/ODM will make changes, but:

• Designers don’t get the source
• Designers can’t change the binary
• Designers can’t ship binary as-is
Enabling Firmware for Derivative Designs

What about things on the Internet?

- Intel® Galileo & Intel® Quark™ technologies
- Uses open source firmware from Intel® UEFI Development Kit 2010 & 2014
- UEFI projects, can be used as-is

But, if firmware changes are needed:

- No tools to help with UEFI porting
- Developer needs UEFI experience
Providing Additional Options for Intel® Architecture (IA) Firmware

New Intel® Architecture (IA) customers have different firmware needs ...

• Firmware is used for product enabling, not product differentiation
• Reference design must enable basic firmware development

How can Intel increase velocity from reference design to product?

• Quickly generate derivative firmware based on reference design
• Increase ease-of-use in firmware development
• Remove firmware experience as a barrier to product deployment

Firmware enabling must address new markets
Agenda

• Firmware Challenges

• Intel® Unified Binary Management Suite (Intel® UBMS)

• Use Cases for Intel UBMS

• Intel UBMS Ecosystem

• Summary / Call to Action
Intel® Unified Binary Management Suite (Intel® UBMS)

Develop derivative platform firmware using modular binary components

• Not “yet another codebase” ... leverages UEFI & Intel® UDK2014
• Based on UEFI v2.4, UEFI PI v1.3 & UEFI PI Distribution Packaging v1.2
• Compatible with existing UEFI Device Drivers (Intel & 3rd party)

Advantages:

• Platform firmware starts from validated reference code
• Platforms use a catalog of compatible components (Intel & 3rd party)
• Widen Intel® Architecture (IA) customer base by simplifying platform firmware
Leveraging UEFI Build Process & Tools

Intel® UEFI Development Kit 2014 (Intel® UDK2014) firmware images aren’t monolithic binaries ...

Parse all package files
Generate makefiles for each module
Compile source for each module
Generate binaries
Group binaries in Firmware Volumes (FV)
Generate firmware device (FD) image from FVs
Extending Intel® UDK2014 with Intel® UBMS

Intel® UBMS extends Intel® UDK2014 to work directly with binaries

- Parse all package files
- Generate makefiles for each module
- Compile source for each module
- Generate binaries
- Group binaries in Firmware Volumes (FV)
- Generate firmware device (FD) image from FVs

Platform repository based on pre-compiled packages
Source compilation replaced with configurable packages
Simplified Configuration

Platform repository based on pre-compiled Intel® UBMS packages
• Add/configure/remove packages
• Add/remove UEFI Drivers

Feature-based approach
• Packages represent hardware capabilities & software features
• Behind-the-scenes configuration
Development Process Using Intel® UBMS

1. Start New Project Based on Reference
2. Change Peripherals & Connectors
3. Configure Firmware Components
4. Generate New Firmware Image
Enabling Multiple Paths for Intel® Architecture Firmware

Intel® Unified Binary Management Suite (Intel® UBMS) changes the enabling model for derivative products

• Fast path from reference design to product
• Quickly generate firmware for simple derivative products

Simplifies development using existing UEFI components

• Tool-based firmware configuration, without need for source code
• Developers do not require experience with Intel® Architecture (IA) firmware

Intel® UBMS adds a new enabling path for IA firmware
Agenda

- Firmware Challenges
- Intel® Unified Binary Management Suite (Intel® UBMS)
- Use Cases for Intel UBMS
- Intel UBMS Ecosystem
- Summary / Call to Action
Use Cases for Intel® UBMS

Simple changes from reference platform to derivative product

- Configure firmware features, based on product changes
- Add/remove firmware features not found in reference platform
- Add 3rd party components not provided with reference platform
Example: Enable Firmware Debug Console

1. Pick ‘Debugger Tool Console’ option from peripherals list
Example: Enable Firmware Debug Console

1. Pick ‘Debugger Tool Console’ option from peripherals list
2. Drag onto project workspace
   - User interface shows peripherals & connectors that are compatible with the feature (in orange)
Example: Enable Firmware Debug Console

1. Pick ‘Debugger Tool Console’ option from peripherals list
2. Drag onto project workspace
   - User interface shows peripherals & connectors that are compatible with the feature (in orange)
3. Debugging is now in the project
Example: Enable Firmware Debug Console

1. Pick ‘Debugger Tool Console’ option from peripherals list
2. Drag onto project workspace
   - User interface will show which peripherals/connectors are compatible with the feature
3. Debugging is now in the project
4. Feature can be configured
Example: Enable Firmware Debug Console

1. Pick ‘Debugger Tool Console’ option from peripherals list
2. Drag onto project workspace
   - User interface will show which peripherals/connectors are compatible with the feature
3. Debugging is now in the project
4. Feature can be configured
5. Build a new firmware image

Intel® UBMS simplifies firmware construction
Agenda

- Firmware Challenges
- Intel® Unified Binary Management Suite (Intel® UBMS)
- Use Cases for Intel UBMS
- Intel UBMS Ecosystem
- Summary / Call to Action
Intel® Unified Binary Management Suite Ecosystem

Intel® Unified Binary Management Suite (Intel® UBMS)
- Build & configure derivative firmware images, based on repository packages
- Target Audience: customer developing derivative firmware for their platform

Package Development Kit (PDK) for Intel UBMS
- Update existing Intel UDK2010 & UDK2014 components to work with Intel UBMS
- Target Audience: Silicon component vendors and firmware developers

Platform Porting Kit (PPK) for Intel UBMS
- Group Intel UBMS compatible binaries into a new platform support set
- Target Audience: System vendors and firmware developers
Creating Packages for Intel® UBMS

Designed to convert existing UEFI code to work with Intel® UBMS

- Intel® UDK2014, Intel® UDK2010 or EDK II codebase (tianocore.org)
- Add metadata via extensions to INF, DEC, DSC & FDF package files
- Exposes Platform Configuration Database (PCD) values to developer as configuration options
- Add Unicode strings (.UNI files) for developer options
Advantages of Intel® UBMS

Extends UEFI capabilities

• Adds configurability to binaries
• Also applies to UEFI Driver Execution Environment (DXE) and Pre-EFI Initialization Modules (PEIM)

Localize configuration strings

Checks for package requirements

• Validate hardware & software requirements before adding
Building the Ecosystem for Intel® UBMS

Intel® Unified Binary Management Suite (Intel® UBMS) is in early development ... but the ecosystem is key

Looking for participation from independent hardware vendors (IHV)

1. If you have code Intel® UDK2014, Intel® UDK2010 or EDK II ... talk to us about converting it to work with Intel UBMS

2. If you have code in EDK 1.06 or earlier ... talk to us about converting it to Intel UDK2014, Intel UDK2010 or EDK II w/o using the EFI Compatibility Package (ECP)

Who do you talk to? Check the “Call to Action” section.

Intel is ready to engage the IHV community and build an ecosystem for Intel UBMS
Agenda

• Firmware Challenges
• Intel® Unified Binary Management Suite (Intel® UBMS)
• Use Cases for Intel UBMS
• Intel UBMS Ecosystem
• Summary / Call to Action
Summary

- Firmware enabling must address new markets
- Intel Unified Binary Management Suite (Intel® UBMS) adds a new enabling path for Intel® Architecture firmware
- Intel UBMS simplifies firmware construction
- Intel is ready to engage the IHV community and build an ecosystem for Intel UBMS
Call to Action

Contact us if you’re interested in working with Intel® Unified Binary Management Suite...

- intel_ubms@intel.com

Make sure your UEFI codebase is using Intel® UDK2014, Intel® UDK2010 or EDK II and is written for “native EDK II”

- No dependency on EFI Compatibility Package (ECP)
Additional Sources of Information

A PDF of this presentation is available from our Technical Session Catalog: www.intel.com/idfsessionsSF. This URL is also printed on the top of Session Agenda Pages in the Pocket Guide.

Information on UEFI for Intel® Architecture available at http://uefidi.com

Intel® UDK2014 and EDK II available at http://tianocore.org

Demos in the showcase – Intel SSG Pavilion Booth #509
Innovation and fun go hand in hand!

• Get your RFID/USB wristband and details at the Software & Services Pavilion in the Technology Showcase, or at our mobile carts outside Moscone West.

• Once you register, you’re connected to:
  - Software and services content
  - Tracking earned coins for the “Surf the Code” game and other prizes
  - Your own 3D avatar with 10 coins… Play the game, share with friends

• Visit the Software & Services Pavilion to earn more coins
  - Talk with Intel experts about your development needs and plans
  - Tinker on your own time with self-run labs, source code, tools
  - Swipe your wristband on the Galileo Scan Stations to get coins

• Play to Win in the Software & Services Pavilion
  - Get 5 coins to play “Surf the Code”… Gift cards for three highest scores!
  - Get 10 coins to get your 3D avatar… And enter daily drawing for tablets and 2-in-1s
  - Get 15 coins for your King Code t-shirt, and increase total game score potential

Don’t let the fun stop!
Daily lunch at food trucks
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 PROPERTY 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.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information. The products described in this document 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. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm

Intel, Look Inside 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. Copyright ©2014 Intel Corporation.
Risk Factors

The above statements and any others in this document that refer to plans and expectations for the second quarter, the year and the future are forward-looking statements that involve a number of risks and uncertainties. Words such as “anticipates,” “expects,” “intends,” “plans,” “believes,” “seeks,” “estimates,” “may,” “will,” “should” and their variations identify forward-looking statements. Statements that refer to or are based on projections, uncertain events or assumptions also identify forward-looking statements. 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 important factors that could cause actual results to differ materially from the company's expectations.

Demand for Intel's products is highly variable and, in recent years, Intel has experienced declining orders in the traditional PC market segment. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions; consumer confidence or income levels; customer acceptance of Intel's and competitors' products; competitive and pricing pressures, including actions taken by competitors; supply constraints and other disruptions affecting customers; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Intel operates in highly competitive industries and its operations have high costs that are either fixed or difficult to reduce in the short term. Intel's 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; segment product mix; the timing and execution of the manufacturing ramp and associated costs; excess or obsolete inventory; changes in unit costs; defects or disruptions in the supply of materials or resources; and product manufacturing quality/yields. Variations in gross margin may also be caused by the timing of Intel product introductions and related expenses, including marketing expenses, and Intel's ability to respond quickly to technological developments and to introduce new products or incorporate new features into existing products, which may result in restructuring and asset impairment charges. Intel's results could be affected 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, divestitures and other significant transactions. 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, disclosure and other issues, such as the litigation and regulatory matters described in Intel's SEC filings. An unfavorable ruling could include monetary damages or an injunction prohibiting Intel 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 company's most recent reports on Form 10-Q, Form 10-K and earnings release.

Rev. 4/15/14