IDF2013
INTEL DEVELOPER FORUM

Using Wind River Simics* Virtual Platforms to Accelerate Firmware Development

Steven Shi, Senior Firmware Engineer, Intel
Chunrong Lai, Software Engineer, Intel
Alexander Y. Belousov, Engineer Manager, Intel

PTAS003

Sponsors of Tomorrow.™ intel

Agenda

- Problems for Today's Firmware Developer
- Benefits of a Virtual Platform
- Using Wind River Simics* for Firmware Development
- Integrating Debug Tools with Wind River Simics
- Summary / Next Steps / Q&A

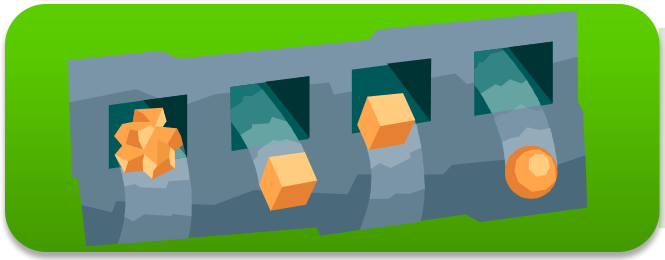
The PDF for this Session presentation is available from our Technical Session Catalog at the end of the day at: intel.com/go/idfsessionsBJ

URL is on top of Session Agenda Pages in Pocket Guide

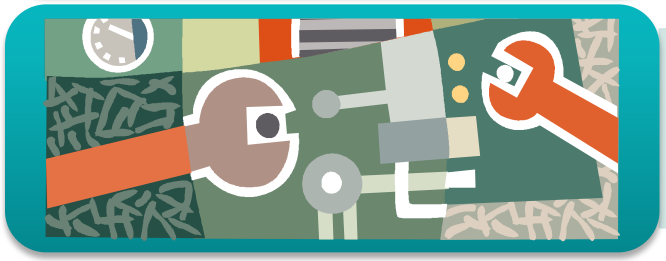

Problems for
Today's Firmware
Developer

Problems for Today's Firmware Developer

Need to work on firmware earlier, especially if hardware is delayed



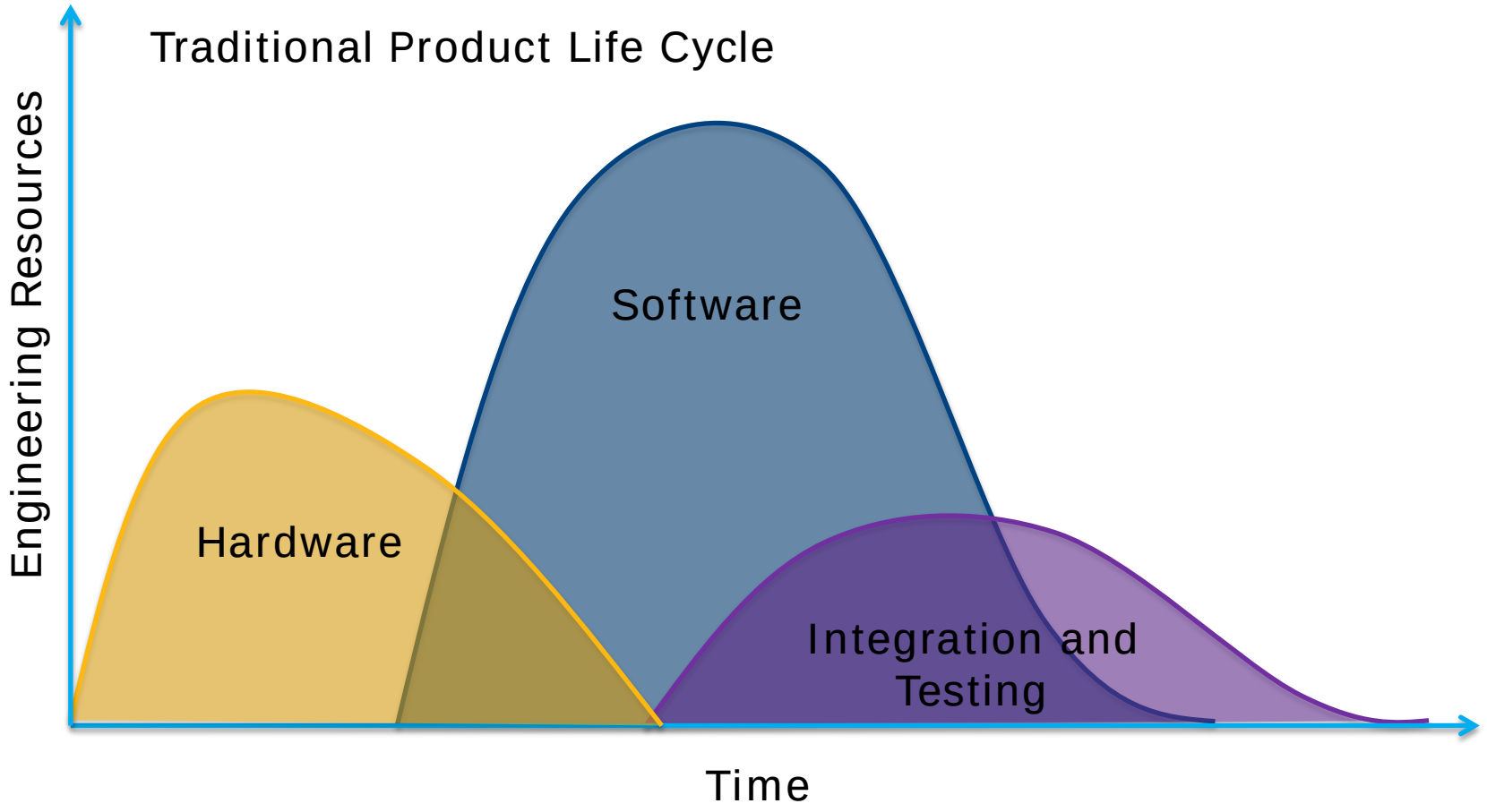
Early boards are missing key features and cannot be tested



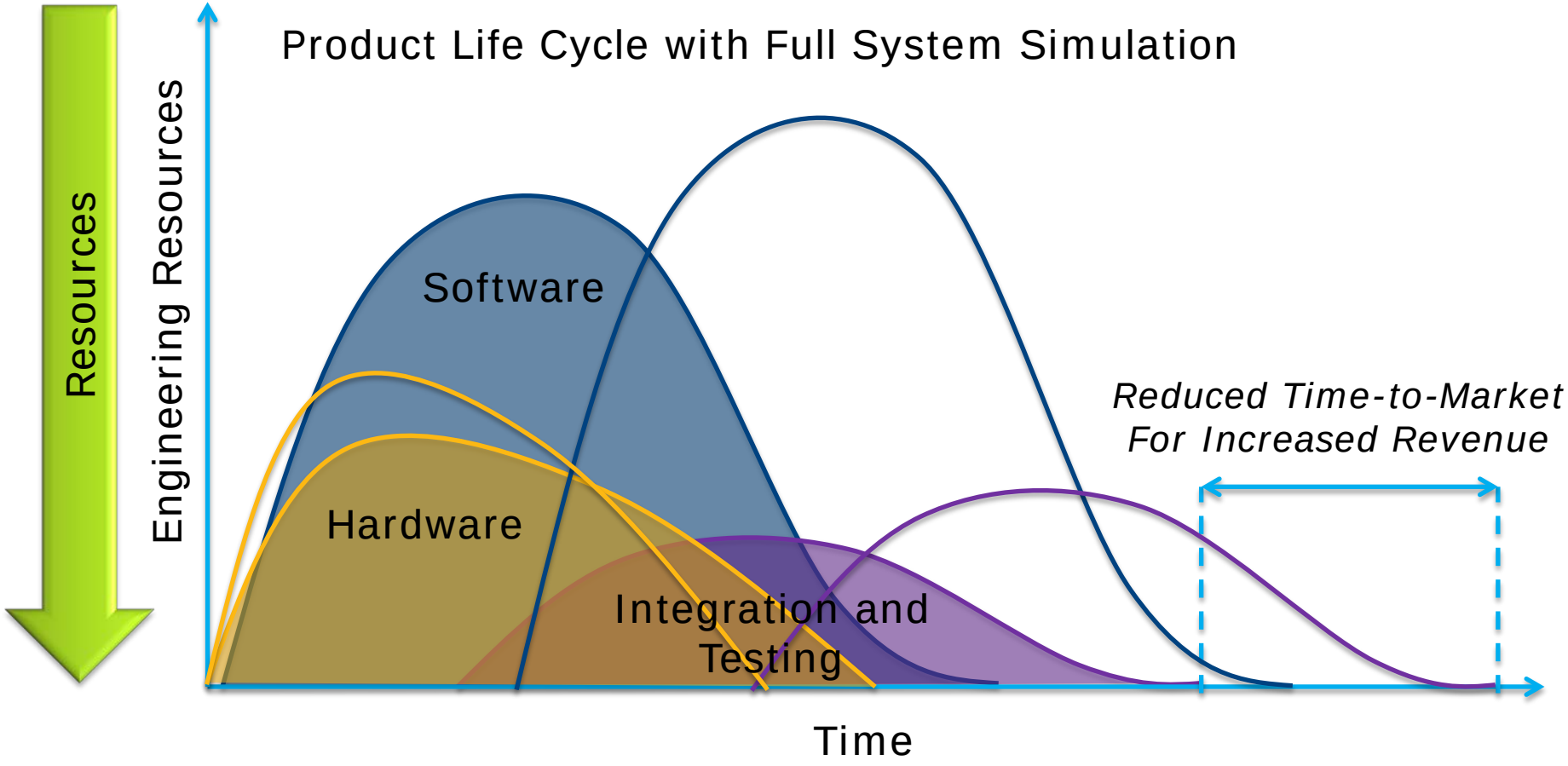
Different configurations cannot be tested using the reference board

Customers need firmware before the board is working

Shift Left: Shorter Time to Market



Shift Left: Shorter Time to Market



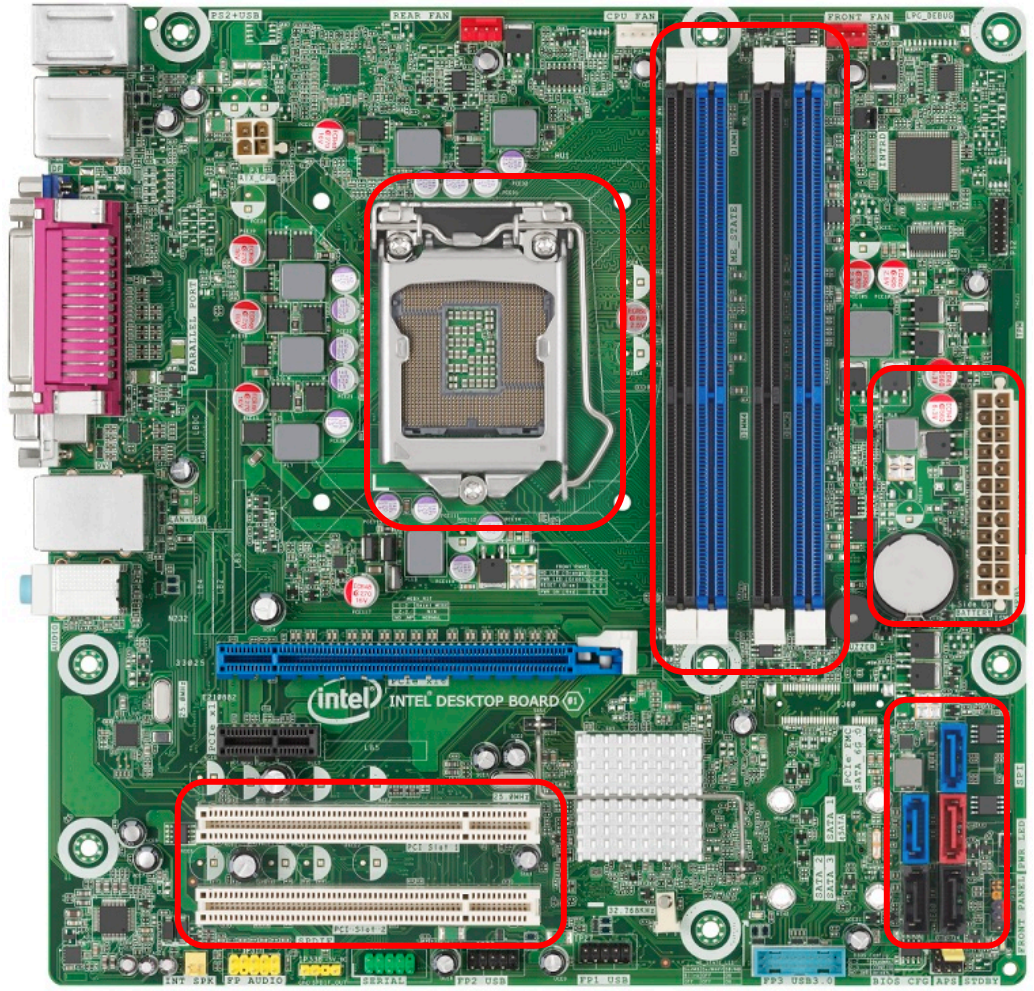
Bringing Up The First Board…

Are all of the ports wired properly?

Can you test against different processor models?

Does the board support the maximum amount of memory?

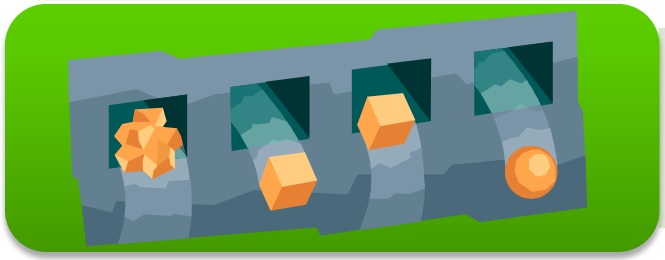
Is the board electrically stable (power, ground, …)?



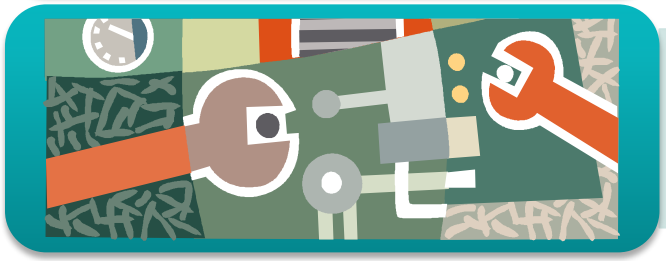
Hardware issues delay firmware delivery

What a Firmware Developer Needs…

- Earlier platform access



- Exercise all platform features



- Quickly try different platform configurations

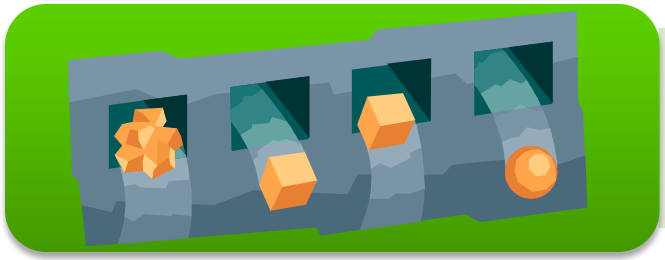
- Work when hardware is unstable or unavailable

Modern firmware needs to go beyond the "reference board"

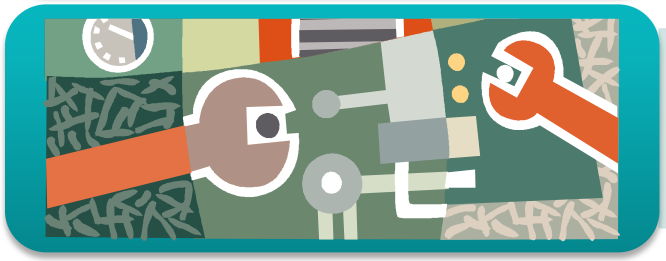
Benefits of a Virtual Platform

Benefits of a Virtual Platform

Available before hardware ships



Models all platform features



Easily reconfigured for testing various platform configurations

Virtual platforms models work even if hardware is unstable

Solving “Classic” Firmware Problems

Virtual platforms address “classic” challenges…

- Customers want boot firmware before the platform is ready
- The first board is always missing key features
- The first board can be unstable and hard to test
- Firmware developers don’t get as many boards as they need

Virtual platform models for Intel® Silicon are available before the reference board

Validate features on a virtual platform before hardware is functional

You don’t “run out” of virtual platforms

Solving “New” Firmware Problems

Reconfigure virtual platforms to include features not found on the reference board

Starting work early on the virtual platform gets the firmware ahead of schedule

People still think this way. We don’t know why. Sorry. ☹

Virtual platforms address other challenges…

- Not every silicon feature can be exercised on the “reference board”
- Customers want to use hardware combinations that can’t be tested on the “reference board”
- Schedules are tighter
- Firmware is “magic” so it will fix everything ☺

Challenges for Virtual Development

Accuracy

- Simulation must model hardware behavior

Performance

- Speed cannot adversely affect development

Debugging

- Similar toolset as used on real hardware

Virtual platforms can benefit firmware development

Using Wind River Simics* for Firmware Development

What Is Wind River Simics*?

Wind River Simics* is a full system simulator used by software developers to simulate the hardware of large and complex electronic systems.

Target system

- Simulate any size of target system
- Run unmodified target binaries

Simics allows you to **break the rules** of product development.

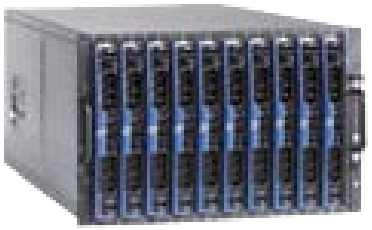
Simulate Electronic System

- Simulate any level of complexity…every engineer ALWAYS has access to the complete system

…or Multiple Boards:
Connected via Ethernet or other communication buses

Simulate A Single Board:
Your own custom board or a standard reference/production board, including CPU and all devices on the board

…or a Rack of Boards:
Connected via VME or other backplane

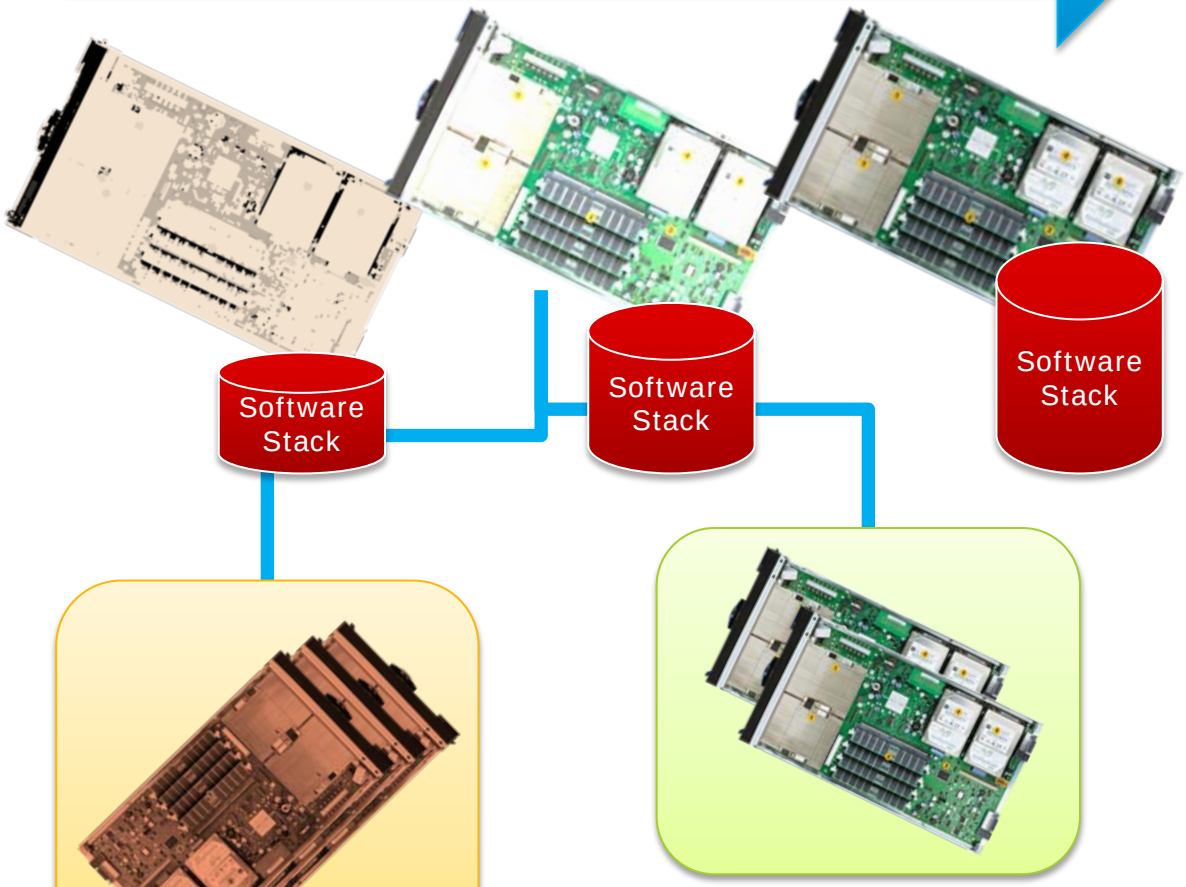


…or your complete customized digital system:
Containing 100's of CPU's and devices




Continuous Integration

No need to delay software development until an SoC or board is fully functional…begin early

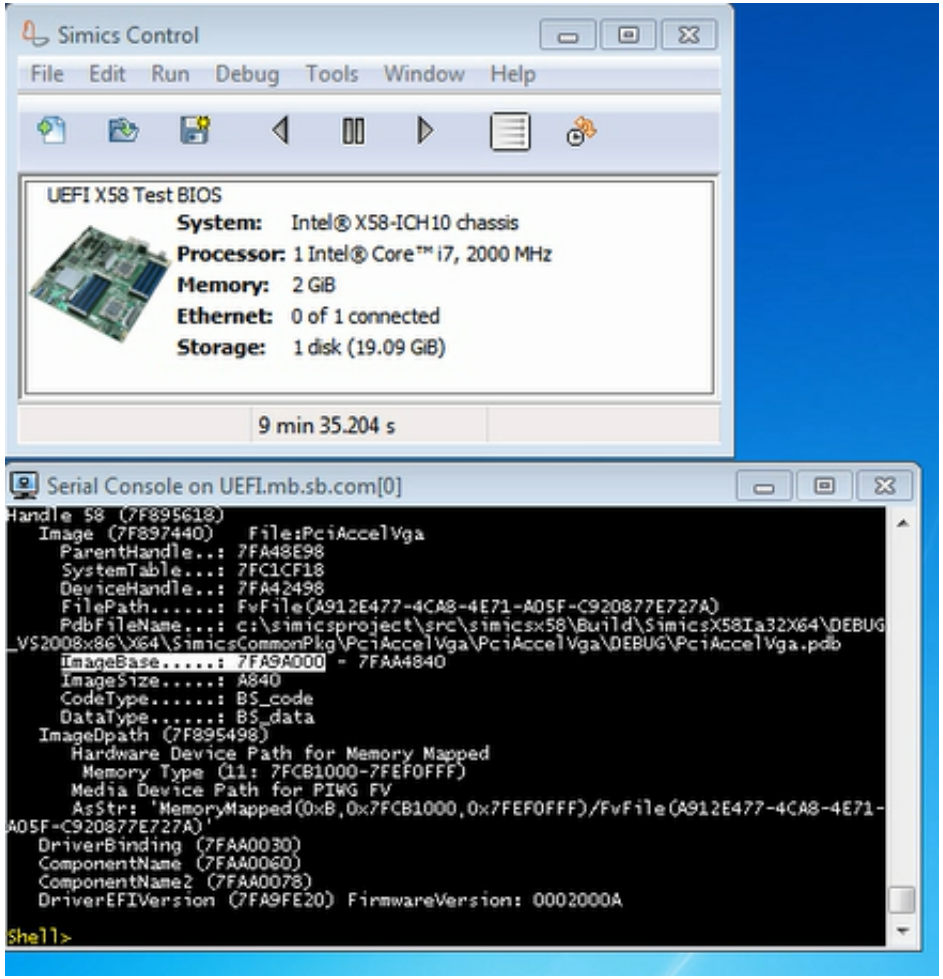


- Integrate throughout the project, don't wait until all hardware is available
- Reduces:
  - Risks
  - Costs
  - Errors
  - Time to market

Begin system integration even before physical components are available

Hardware Accuracy in Simics*

- The accuracy of the Simics* model can be demonstrated with the platform's UEFI BIOS
- *Binary is unmodified between hardware and Simics*
- Code can run without any awareness of the virtual environment



Managing Performance in Simics*

Microsoft* Windows* 7 boots[1] in about **1 minute** on Simics*

Some customer systems take almost 30 minutes to boot (on real hardware)

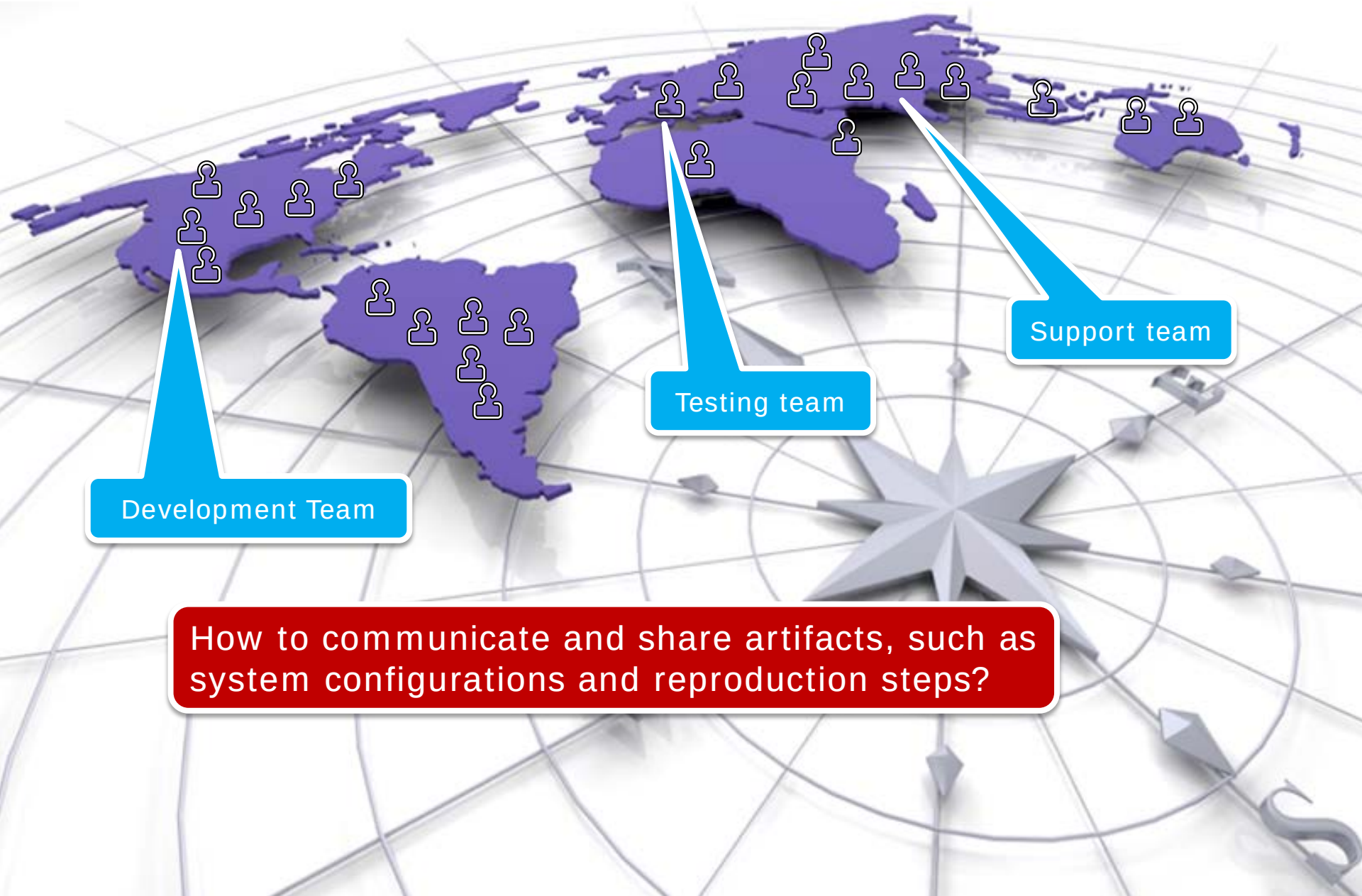
Add to this time for loading applications, running to interesting points, etc.

Microsoft Windows 7 can be restored from a checkpoint in about **1 second**[1]

Loading from checkpoints is even faster than the traditional boot process

[1] Actual boot time will depend on host and target configuration. Results may vary.

Today's Reality: Worldwide Development



How to communicate and share artifacts, such as system configurations and reproduction steps?

Checkpoint Collaboration

Simics* Virtual Platform
Exact configuration of the target system where the bug was found

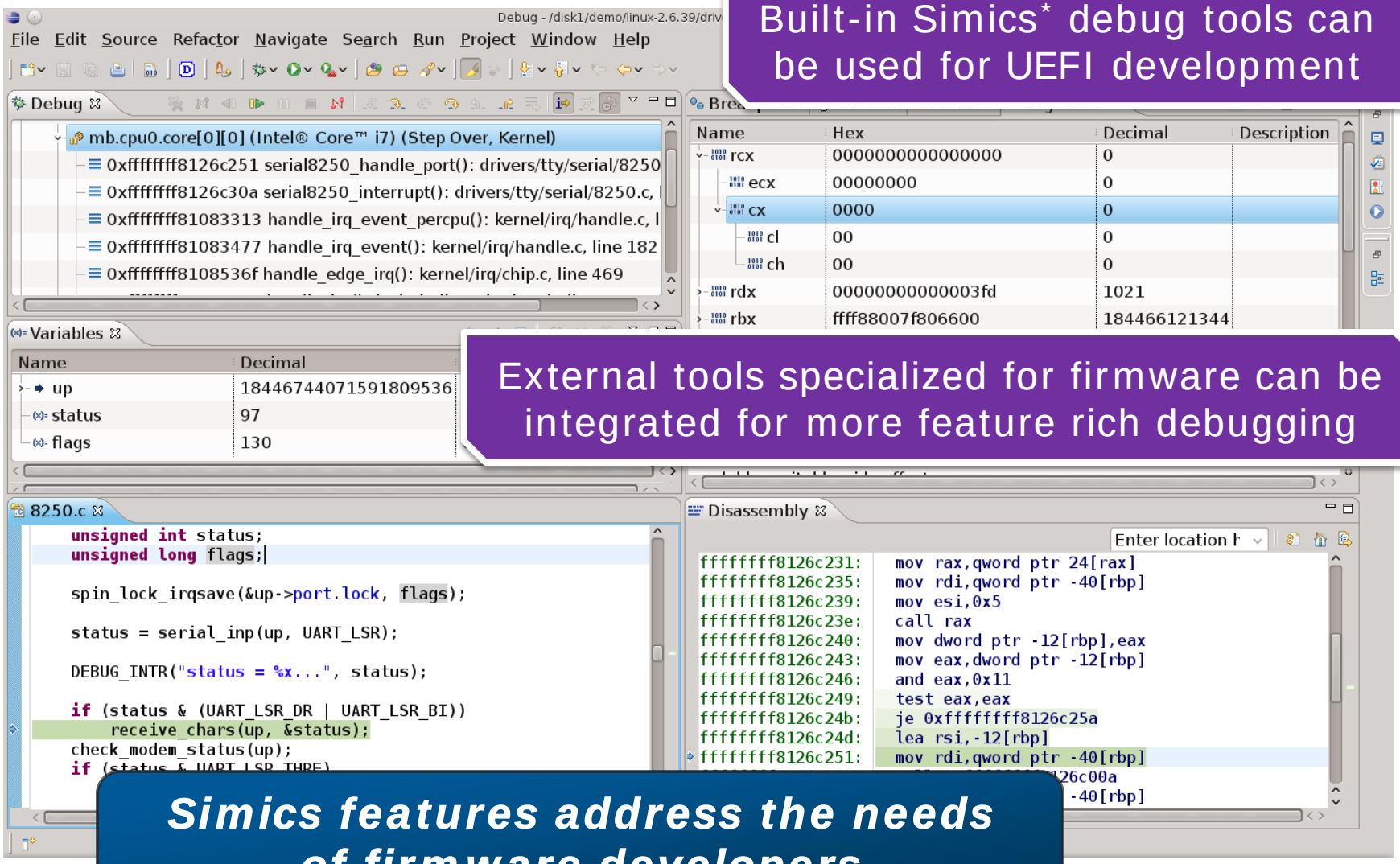
Simics Script
Automate the actions that led to a bug

Simics Checkpoint
A snapshot of the full system that can be restarted on any machine anywhere

Testing Team
Finds a bug

Development Team
Loads checkpoint and resumes execution to find the source of the bug

Software Debugging in Simics*



Feedback from Internal Users:

- Simics* was used for UEFI BIOS development:
  - *"…Various BIOS issues eliminated 3 months before first silicon, only 1 minor BIOS defect caught during hardware bring up"*
  - *"…I would like to say that Simics is a very powerful tool that allows you to do almost any kinds of things/tweaks/hacks/workarounds on the model which I think other simulators not able to offer."*
  - *"…A lot of BIOS bugs being caught during the early stage while using Simics, including the scary ACPI issue. In the end, we still able to get successfully PO with the BIOS with almost no ACPI issue."*


Integrating Debug Tools with Wind River Simics*

Integrating Intel® ITP Software with Wind River Simics*

One example of debug tool integration is using Intel® In-Target Probe (Intel® ITP) software with Simics*

- Same toolset used on physical hardware
- Simple integration with Simics
  (does not rely on Extended Debug Port –XDP interface)

Working Example:

- Boot to UEFI Shell
- Add breakpoint to video driver
- Trace driver through BLT function

Demo Video

UEFI Debug Capacities Integrated in Wind River Simics* Eclipse* Frontend

Video demo:

- Based on Simics* server model of next generation Intel® Microarchitecture codename Haswell
- Set breakpoints proactively, keep them between runs
- Execution control of: step into/over, step out, reverse step into/over, un-call
- Direct source file editing within debugger
- Inspecting of variables, registers and UEFI modules
- Provide access to all generic UEFI commands

Summary

- Modern firmware needs to go beyond the “reference board”
- Virtual platforms can benefit firmware development
- Simics* features address the needs of firmware developers
- Simics offers seamless firmware debugging

Get More Information

UEFI

- UEFI Forum Learning Center
  - http://www.uefi.org/learning_center/
- Intel UEFI Community
  - http://intel.com/udk
- Use the TianoCore edk2-devel mailing list for support from other UEFI developers

Wind River Simics*

- http://www.windriver.com/products/simics/
- http://www.intel.com/p/en_US/embedded/hwsw/software/simics

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.
- Intel product plans in this presentation do not constitute Intel plan of record product roadmaps. Please contact your Intel representative to obtain Intel's current plan of record product roadmaps.
- Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. Go to: http://www.intel.com/products/processor_number.
- 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
- Haswell and other code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user
- Intel, Sponsors of Tomorrow 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.
-

IDF2013
INTEL DEVELOPER FORUM

Legal Disclaimer

- Software Source Code Disclaimer: Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license. {include a copy of the software license, or a hyperlink to its permanent location}
- Other Software Code Disclaimer:
  Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
  THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Risk Factors

The above statements and any others in this document that refer to plans and expectations for the first 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 the important factors that could cause actual results to differ materially from the company’s expectations. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions; customer acceptance of Intel’s and competitors’ products; supply constraints and other disruptions affecting customers; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Uncertainty in global economic and financial conditions poses a risk that consumers and businesses may defer purchases in response to negative financial events, which could negatively affect product demand and other related matters. Intel operates in intensely competitive industries that are characterized by a high percentage of costs that are fixed or difficult to reduce in the short term and product demand that is highly variable and difficult to forecast. Revenue and the gross margin percentage are affected by the timing of Intel product introductions and the demand for and market acceptance of Intel's products; actions taken by Intel's competitors, including product offerings and introductions, marketing programs and pricing pressures and Intel’s response to such actions; and Intel’s ability to respond quickly to technological developments and to incorporate new features into its products. The 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; start-up costs; excess or obsolete inventory; changes in unit costs; defects or disruptions in the supply of materials or resources; product manufacturing quality/yields; and impairments of long-lived assets, including manufacturing, assembly/test and intangible assets. 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. Expenses, particularly certain marketing and compensation expenses, as well as restructuring and asset impairment charges, vary depending on the level of demand for Intel's products and the level of revenue and profits. Intel’s results could be affected by the timing of closing of acquisitions and divestitures. Intel’s current chief executive officer plans to retire in May 2013 and the Board of Directors is working to choose a successor. The succession and transition process may have a direct and/or indirect effect on the business and operations of the company. In connection with the appointment of the new CEO, the company will seek to retain our executive management team (some of whom are being considered for the CEO position), and keep employees focused on achieving the company’s strategic goals and objectives. 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 reports. 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 Form 10-Q, report on Form 10-K and earnings release.

Rev. 1/17/13

IDF2013
INTEL DEVELOPER FORUM

Using Wind River Simics* Virtual Platforms to Accelerate Firmware Development

Backup Materials

Sponsors of Tomorrow.™ intel

Problems for Today's Firmware Developer

The "classic" challenges haven't changed…

- Customers want boot firmware before the platform is ready
- The first board is always missing key features
- The first board can be unstable and hard to test
- Firmware developers don't get as many boards as they need

Over time, we have more interesting challenges…

- Not every silicon feature can be exercised on the "reference board"
- Customers want to use hardware combinations that can't be tested on the "reference board"
- Schedules are tighter
- Firmware is "magic" so it will fix everything ☺

Benefits Going Virtual

Hardware

- Actual behavior
- Speed

Simulator

- Non-intrusive debugging
- Checkpointing
- Determinism
- Reverse execution
- Scripting
- Hardware replication
- Speed!

Speed? Really?

- Embedded processors slower than server ones
- Almost reach host speed for x86 on x86 (VMP)
- Complex systems often boot slowly
  - Waiting for slow hardware, mandatory timeouts
  - Clearing memory
  - Hardware self-tests
  - Lots of idle time in parallel systems
- Simics can fast forward when system is waiting!
- Loading software on real system:
  - Program flash memory, load over network or USB
- Loading software on Simics*:
  - Load binary directly into target memory in no time
- Checkpointing
  - No need to reboot every time