IDF2013
英特尔信息技术峰会

使用 Wind River Simics* 虚拟平台加速固件开发

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

PTAS003

英特尔®与你共创明天™ intel®

议程

- 当前固件(firmware)开发的问题
- 虚拟平台的优势
- Wind River （风河） Simics* 在固件开发中的应用
- Wind River （风河） Simics* 集成的调试功能
- 总结 / 问答

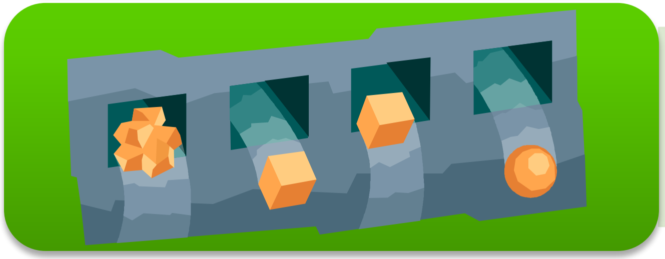
本课程演示文稿（PDF）发布在技术课程目录网站:
intel.com/go/idfsessionsBJ

该网址同时打印于会议指南中专题讲座日程页的上方

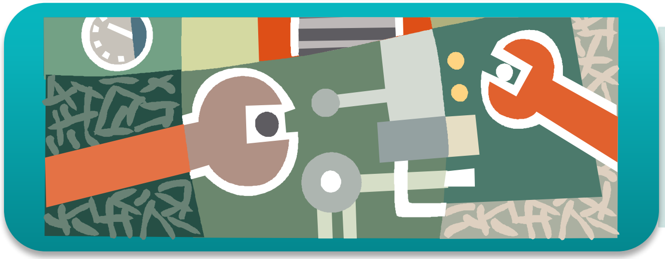
当前
固件开发
的问题

当前固件(firmware)开发的问题

需要更早地进行固件开发
特别在硬件延迟的情况下



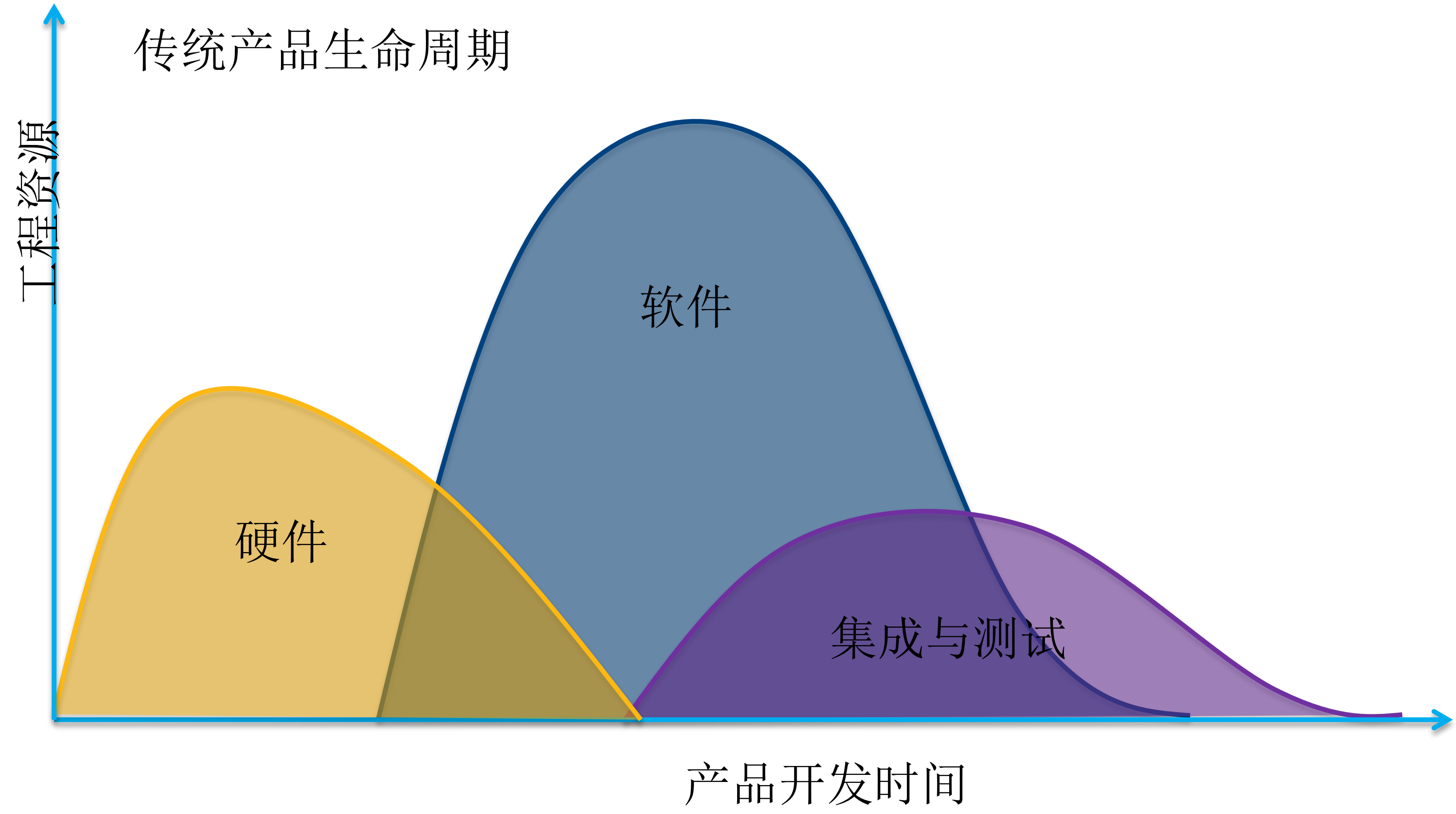
早期的参考板部分关键功能缺失.
难以测试



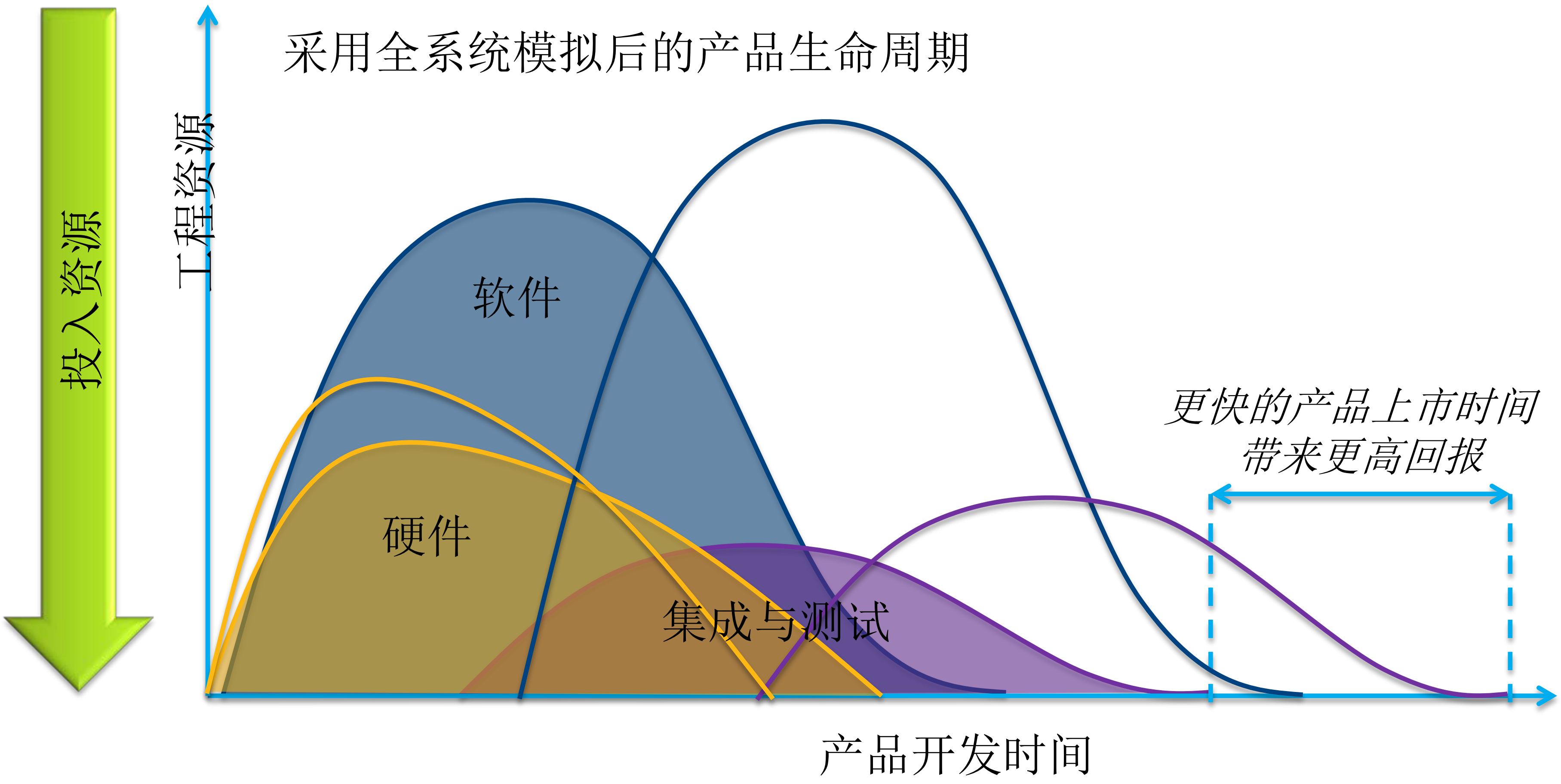
参考板无法修改关键配置
以作固件测试

参考板功能尚未稳定
客户即已要求完整固件

左移：加快产品上市速度



左移：加快产品上市速度



IDF2013
英特尔信息技术峰会

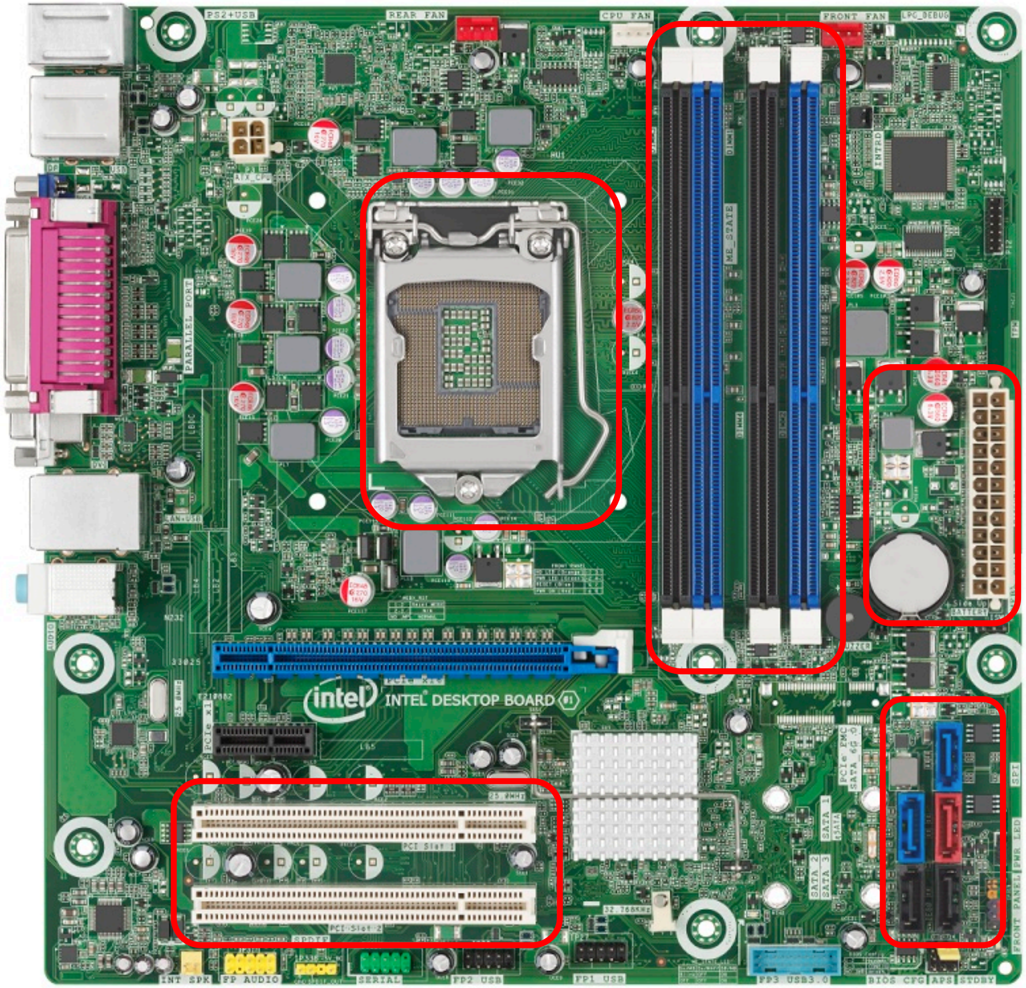
启动第一块单板…

所有端口连线无误?

能测试不同的处理器?

该单板能支持不同大小,
如：最大容量，的内存?

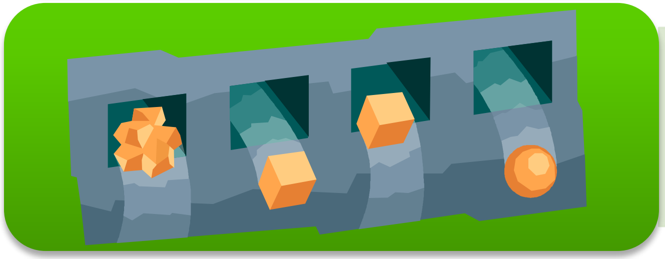
逻辑电平状态稳定
(电压，地线，校准线)?



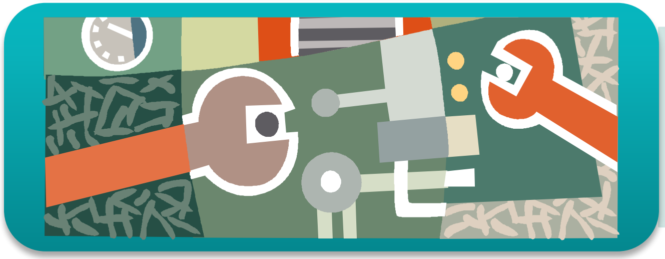
硬件问题往往延迟固件发布

固件开发者需要的是…

- 更早可用的平台



- 能运行所有平台特性



- 快速尝试不同平台配置

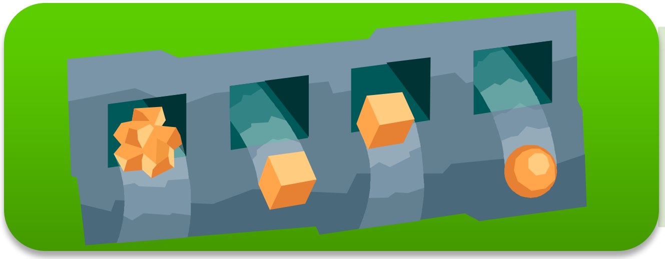
- 即使硬件不稳定或不可用， 也不影响工作

现代固件开发需要超越 “参考板”

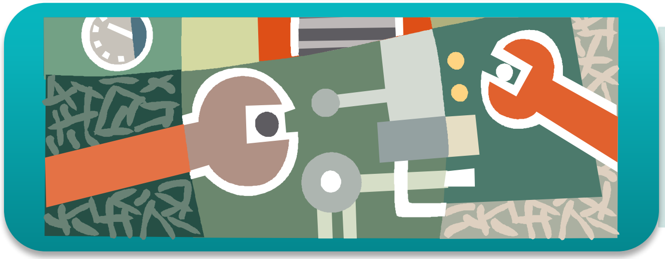
虚拟平台的优势

虚拟平台的优势

在硬件正式发行前即可用



对所有平台特性建模



通过脚本方便地重配置系统， 并进行对各种配置系统的模拟与测试

虚拟平台总是提供稳定的执行环境与可重现的执行结果

解决 “经典” 固件问题

虚拟平台可处理 “经典” 问题 …

- 用户希望在硬件平台可用之前启动固件
- 第一块单板总有关键功能或特性缺失
- 第一块单板往往不稳定而难以测试
- 早期单板数量有限，难以满足系统固件开发的需要

对英特尔硬件建模的虚拟平台在参考板之前即可用于软件开发

在硬件稳定之前虚拟平台已实现稳定有效的相关特性

虚拟平台实际作为软件使用没有数量限制

解决 “新” 固件问题

通过虚拟平台处理其它问题…

- 并非每个硬件特性在参考板上皆可运行
- 用户想尝试参考板中并未包含的硬件组合.
- 固件开发周期要求过紧
- 固件就是“魔法”. 她能解决一切问题 ☺

重配置虚拟平台来包含虚拟板中未实现的特性

利用虚拟平台更早进行固件开发

许多人还是会这么想, 我们不知道为什么 ☹

通过虚拟平台开发的难点

精确度

- 模拟器需要正确建模硬件行为

性能

- 不能因为模拟硬件速度过慢反而影响开发

调试能力

- 是否提供真实硬件上相应的调试工具与调试能力

虚拟平台能益于固件开发

风河Simics* 在固件开发中的应用

风河(Wind River)Simics*是怎样一个工具?

风河Simics*是一个全系统软件模拟器，供软件开发者模拟硬件，她能模拟任何规模和复杂度的电子系统。

目标系统

- 模拟任何规模的目标系统
- 运行无需修改的目标代码

Simics*帮您突破传统的产品开发流程

能模拟任何电子系统

- （软件）模拟使工程师人手一套系统，不管它多复杂…

…或多板：
通过以太网或其他总线互联

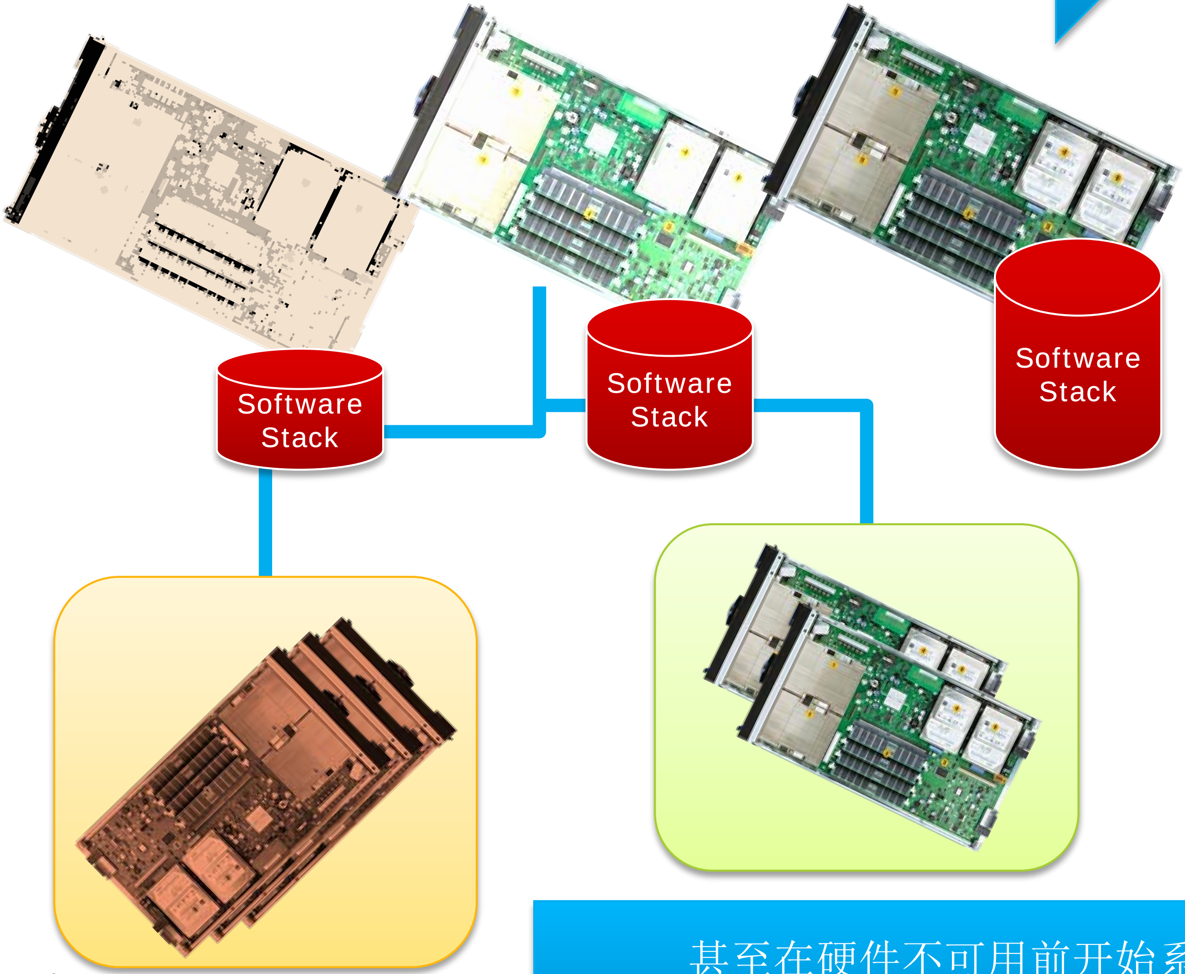
…或整个机架：
通过VME或背板互联

…或是定制的完整数字系统：
包括上百个CPU和外设

模拟单板：
客户定制板
或标准成品/参考设计板，
包含CPU和板上所有外设

持续集成

不必推迟软件开发以等待芯片或新板全部完工…
更早开始



- 全项目周期的持续集成，不用等待硬件
- 减少（小）：
  - 风险
  - 费用
  - 失误
  - 产品上市时间

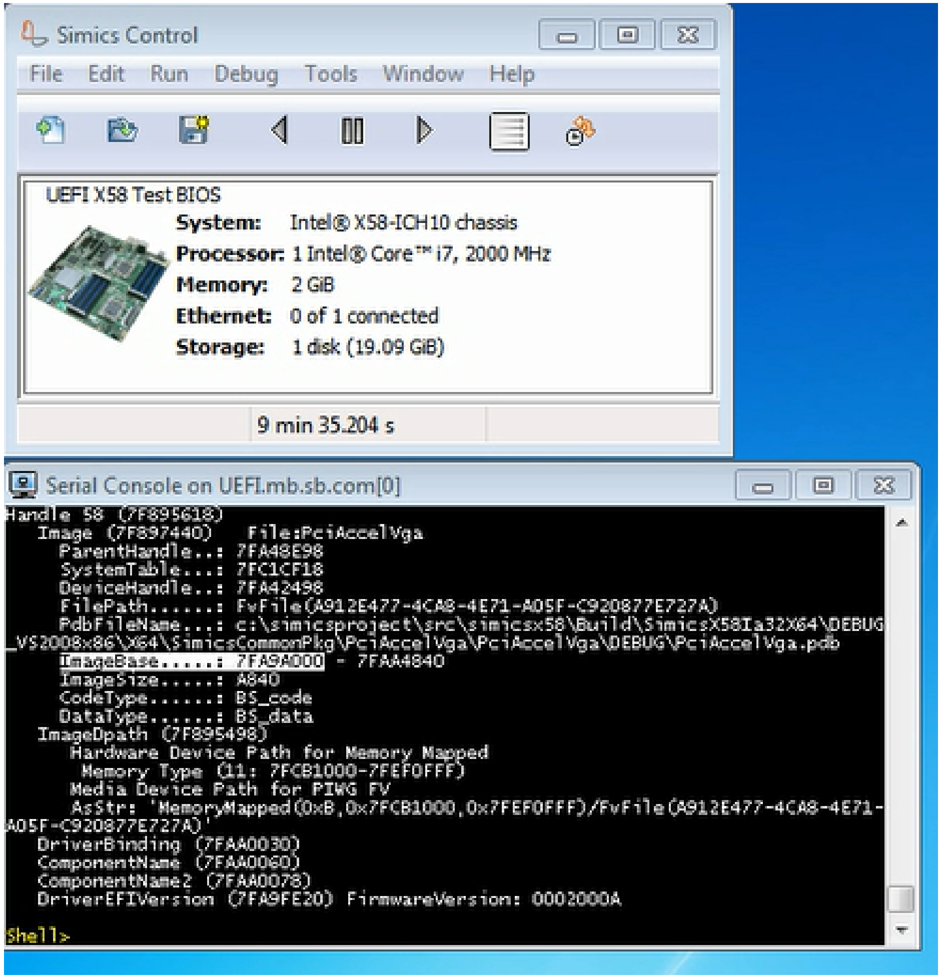
甚至在硬件不可用前开始系统集成

Simics* 的硬件模拟精度

- Simics* 模型的精确度能用模拟硬件平台上运行的UEFI BIOS 来展示

- *在真实与模拟硬件平台间, 目标代码无需修改*

- 目标代码甚至不知道自己是在模拟器上运行



UEFI X58 Test BIOS

System: Intel® X58-ICH10 chassis
Processor: 1 Intel® Core™ i7, 2000 MHz
Memory: 2 GiB
Ethernet: 0 of 1 connected
Storage: 1 disk (19.09 GiB)

9 min 35.204 s

```
Handle 58 (7F895618)
   Image (7F897440)    File:PciAccelVga
     ParentHandle..: 7FA48E98
     SystemTable...: 7FC1CF18
     DeviceHandle..: 7FA42498
     FilePath......: FvFile(A912E477-4CA8-4E71-A05F-C920877E727A)
     PdbFileName...: c:\simicsproject\src\simicsx58\Build\SimicsX58Ia32X64\DEBUG
_VS2008x86\X64\SimicsCommonPkg\PciAccelVga\PciAccelVga\DEBUG\PciAccelVga.pdb
     ImageBase.....: 7FA9A000 - 7FAA4840
     ImageSize.....: A840
     CodeType......: BS_code
     DataType......: BS_data
   ImageDpath (7F895498)
      Hardware Device Path for Memory Mapped
       Memory Type (11: 7FCB1000-7FEF0FFF)
      Media Device Path for PIWG FV
      AsStr: 'MemoryMapped(0xB,0x7FCB1000,0x7FEF0FFF)/FvFile(A912E477-4CA8-4E71-
A05F-C920877E727A)'
   DriverBinding (7FAA0030)
   ComponentName (7FAA0060)
   ComponentName2 (7FAA0078)
   DriverEFIVersion (7FA9FE20) FirmwareVersion: 0002000A

Shell>
```

Simics* 模拟运行速度

在 Simics* 模拟硬件上，Microsoft* Windows* 7 实际启动[1] 时间约 1 分钟

Simics Console: win_viper.console.con - Press shift and right button to enable mouse input
Control Panel
Search Control Panel
View by: Category
Getting Started
Connect to a Projector
Calculator
Sticky Notes
Snipping Tool
Paint
XPS Viewer
Windows Fax and Scan
Remote Desktop Connection
Windows Memory Diagnostic
All Programs
Search programs and files
Simics
Documents
Pictures
Music
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support
Shut down
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display

真实硬件上某些用户系统启动windows 7时间甚至接近30分钟

用户还需要更多时间运行指定应用到相关场景

Microsoft Windows 7 能只用约1 秒[1] 即从系统检查点(checkpoint) 恢复

从Simics* 系统检查点中恢复甚至比传统启动过程更快

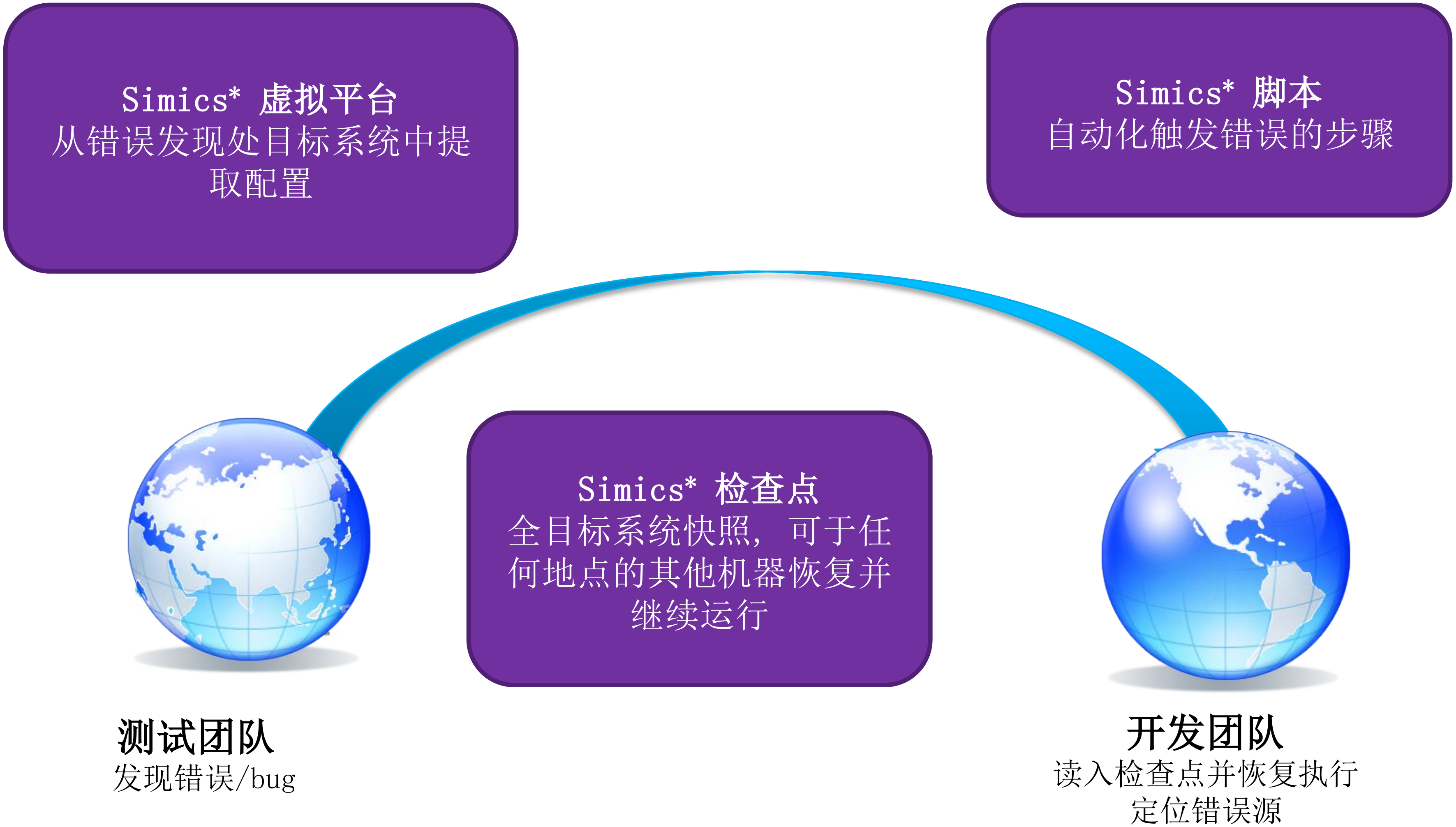
[1] 实际启动时间依赖于宿主机资源与所模拟硬件配置. 配置不同结果可能亦不同.

今日现实：系统开发全球化

开发团队
测试团队
支持团队
S

如何准确地交流与分享事务，例如系统配置与场景重现步骤？

基于系统检查点(Checkpoint)协同工作



Simics* 虚拟平台
从错误发现处目标系统中提取配置

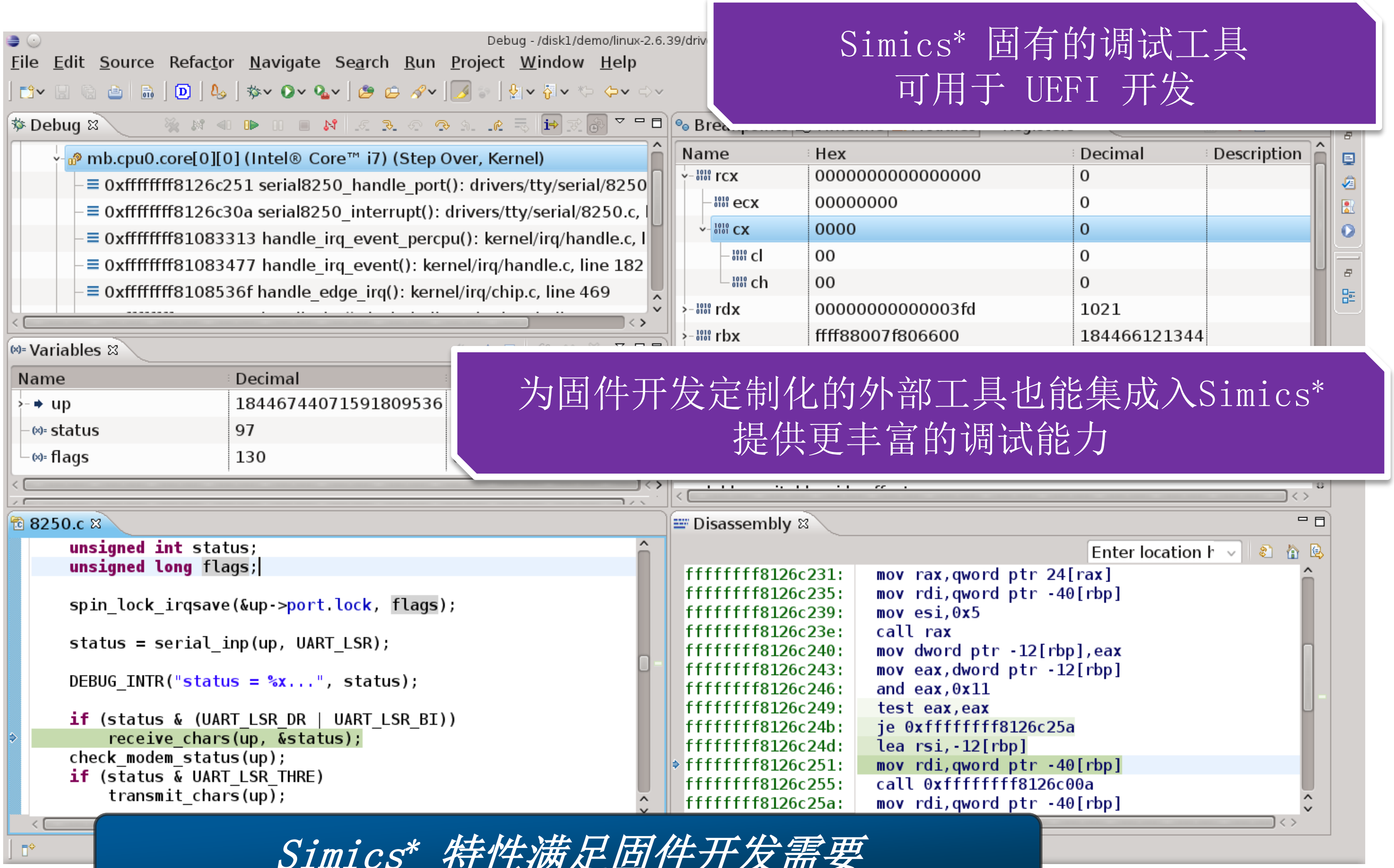
Simics* 脚本
自动化触发错误的步骤

Simics* 检查点
全目标系统快照，可于任何地点的其他机器恢复并继续运行

测试团队
发现错误/bug

开发团队
读入检查点并恢复执行
定位错误源

在Simics*虚拟平台中调试软件



```
mb.cpu0.core[0][0] (Intel® Core™ i7) (Step Over, Kernel)
  0xffffffff8126c251 serial8250_handle_port(): drivers/tty/serial/8250
  0xffffffff8126c30a serial8250_interrupt(): drivers/tty/serial/8250.c, l
  0xffffffff81083313 handle_irq_event_percpu(): kernel/irq/handle.c, l
  0xffffffff81083477 handle_irq_event(): kernel/irq/handle.c, line 182
  0xffffffff8108536f handle_edge_irq(): kernel/irq/chip.c, line 469
```

Name	Hex	Decimal	Description
rcx	0000000000000000	0	
ecx	00000000	0	
cx	0000	0	
cl	00	0	
ch	00	0	
rdx	00000000000003fd	1021	
rbx	ffff88007f806600	184466121344	

Name	Decimal
up	18446744071591809536
status	97
flags	130

```
	unsigned int status;
	unsigned long flags;

	spin_lock_irqsave(&up->port.lock, flags);

	status = serial_inp(up, UART_LSR);

	DEBUG_INTR("status = %x...", status);

	if (status & (UART_LSR_DR | UART_LSR_BI))
		receive_chars(up, &status);
	check_modem_status(up);
	if (status & UART_LSR_THRE)
		transmit_chars(up);
```

```
ffffffff8126c231:   mov rax,qword ptr 24[rax]
ffffffff8126c235:   mov rdi,qword ptr -40[rbp]
ffffffff8126c239:   mov esi,0x5
ffffffff8126c23e:   call rax
ffffffff8126c240:   mov dword ptr -12[rbp],eax
ffffffff8126c243:   mov eax,dword ptr -12[rbp]
ffffffff8126c246:   and eax,0x11
ffffffff8126c249:   test eax,eax
ffffffff8126c24b:   je 0xffffffff8126c25a
ffffffff8126c24d:   lea rsi,-12[rbp]
ffffffff8126c251:   mov rdi,qword ptr -40[rbp]
ffffffff8126c255:   call 0xffffffff8126c00a
ffffffff8126c25a:   mov rdi,qword ptr -40[rbp]
```

Simics* 固有的调试工具
可用于 UEFI 开发

为固件开发定制化的外部工具也能集成入Simics*
提供更丰富的调试能力

Simics 特性满足固件开发需要*

内部用户使用反馈:

- Simics* 已被用于UEFI BIOS开发:
  - *“… 在使用第一块硬件单板之前三个月就已经被发现和消除了许多BIOS问题，启动那块单板只遇到了一个较小的BIOS软件错误”*
  - *“… Simics是非常强大的工具，她允许用户对模型和软件做几乎任何调试/修改/替代方案，其它模拟器很难做到”*
  - *“… 通过Simics在更早的阶段触发并修正了许多BIOS的软件错误，包括一些复杂的ACPI问题，使用几乎没有ACPI问题的BIOS终于能成功地对项目进行立项. ”*

风河 Simics*
集成的调试功能

风河Simics* 集成英特尔® ITP 软件

作为例子，Simics* 集成了英特尔® ITP(In-Target Probe)软件调试工具

- 与真实硬件使用相同的工具界面/前端
- 工具后端直接使用Simics*固有的调试功能
  (并不依赖或需要模拟扩展调试端口 - XDP 硬件接口)

示范视频:

- 启动到UEFI Shell
- 在视频驱动程序中添加断点
- 调试驱动程序中的 BLT 函数

Demo Video

IDF2013
英特尔信息技术峰会

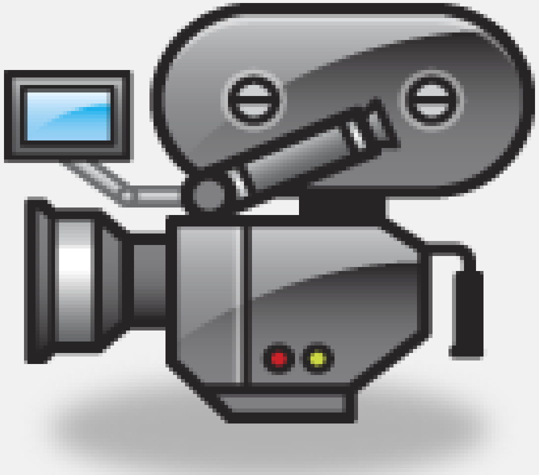
在风河Simics* Eclipse* 界面中集成UEFI 调试能力

示范视频:

- 视频用例运行于基于英特尔下一代微架构(codename Haswell)的Simics*服务器模型
- 自由设置各类断点, 不受动态模块调用与多遍运行影响.
- 提供执行控制: 单步, 单步跨过(step over), 函数跳过(step out), 逆向单步, 逆向单步跨过, 逆向函数跳过(un-call)
- 调试器内直接源文件编辑
- 检查与调试各种软件变量,硬件寄存器,

  以及UEFI模块
- 可访问所有通用UEFI命令

Demo Video



总结

- 现代固件开发需要超越“参考板”
- 虚拟平台能益于固件开发
- Simics* 特性满足固件开发需要
- Simics* 提供无缝固件调试

更多信息

UEFI

- UEFI 论坛学习中心
  - http://www.uefi.org/learning_center/
- 英特尔UEFI 社区
  - http://intel.com/udk
- 使用TianoCore edk2-devel mailing list 邮件列表得到其它UEFI开发者帮助

风河 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.
-

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
英特尔信息技术峰会

使用 Wind River Simics* 虚拟平台加速固件开发

Backup Materials

英特尔®与你共创明天™ 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 ☺

虚拟化后的益处

真实硬件

- 真实行为
- (通常)更快的执行速度

模拟器

- 自由调试
- Checkpointing(系统检查点/快照)
- 执行确定性
- 可逆执行
- 脚本控制
- 替代硬件
- 优化的执行速度

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