IDF16
英特尔信息技术峰会

使用 UEFI 高级功能加速固件开发

魏东
副总裁兼院士, HPE
叶婷
UEFI固件架构师, 英特尔

STTS001

intel
experience
what's inside™

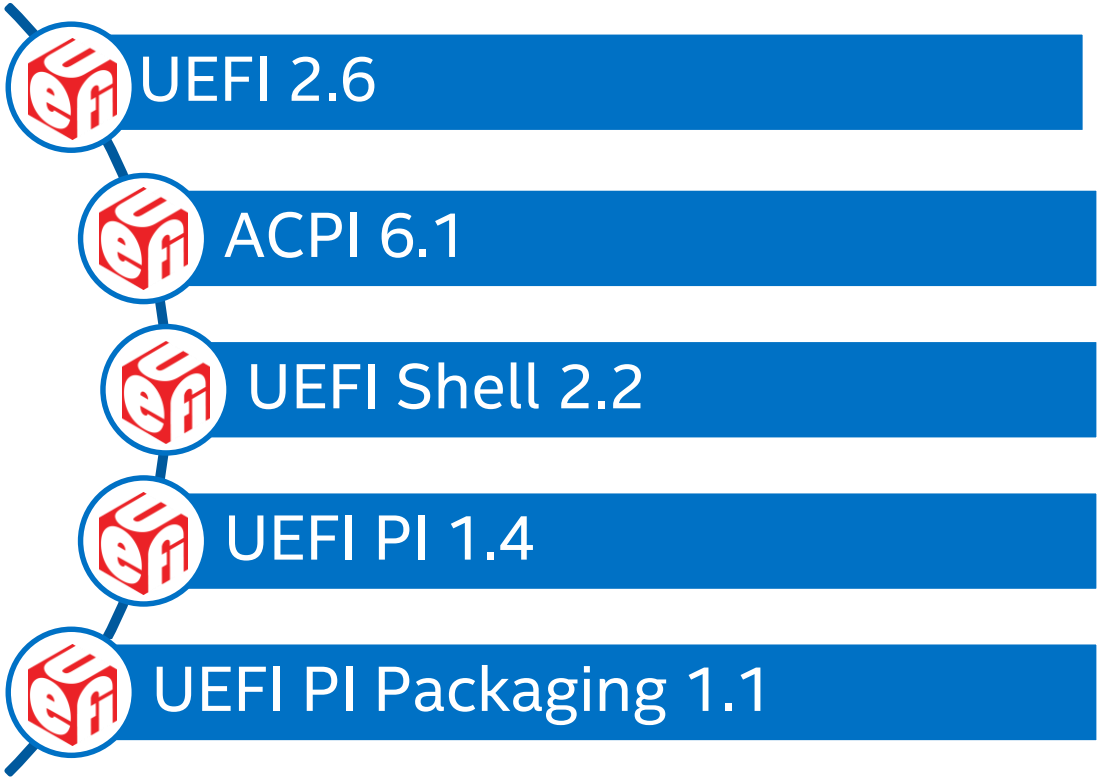
议程

- UEFI和ACPI技术规范的最新信息
- Redfish RESTful技术在数据中心的应用范例
- UEFI核心功能应用于UEFI开发
- 总结

议程

- UEFI和ACPI技术规范的最新信息
- Redfish RESTful技术在数据中心的应用范例
- UEFI核心功能应用于UEFI开发
- 总结

UEFI和ACPI技术规范的最新版本



http://uefi.org/specifications

UEFI 2.5 已定义的网络技术

- HTTP(S) 网络启动 (HTTP 接口, HTTP 辅助型接口, DNS v4/v6, RAMDISK, …)
- Wi-Fi (EAP，可扩展认证协议)
- TLS, 安全传输层协议
- 蓝牙®
- Redfish REST 协议

www.uefi.org

UEFI 2.6规范的更新

网络相关

- Wireless MAC Connection II 协议
- RAMDISK 协议

RAS相关

- CPER (通用型平台出错记录技术) 针对ARM*所做的扩展

HII相关

- 人机接口框架 (HII) Font Ex, Glyph Generator, Image Ex and Image Generator 等协议

I/O相关

- SD/eMMC Pass Thru协议
- PCI Root Bridge和I/O协议支持Non-identity地址映射

www.uefi.org

ACPI 6.1规范的更新

持久性内存相关

- NFIT更新
- NFIT根设备 _DSM

RAS相关

- APEI针对ARM* 所做的扩展
- ERST/EINJ 最大等待时长

管理相关

- Graceful Shutdown技术的说明
- 无线功率校准装置

I/O相关

- 支持利用中断通知的事件

UEFI和ACPI规范的更新有助于加速固件开发

www.uefi.org

议程

- UEFI和ACPI技术规范的最新信息
- Redfish RESTful技术在数据中心的应用范例
- UEFI核心功能应用于UEFI开发
- 总结

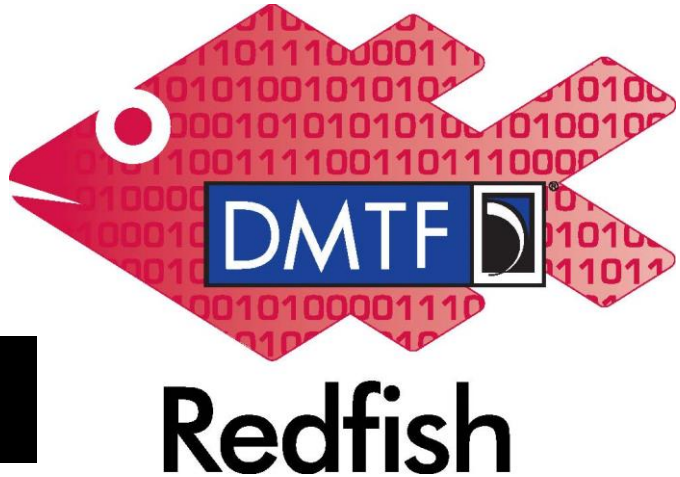
Redfish RESTful技术应用于数据中心的实用范例

什么是 Redfish?

- 业界标准 - www.dmtf.org/standards/redfish
- DMTF* SPMF (可扩展平台管理论坛) 提供技术规范、模式、模型、白皮书、常见问题解答以及资源浏览器

通过RESTful接口管理多代码服务器

- 基于现代工具链(HTTPS, JSON, OData)构建



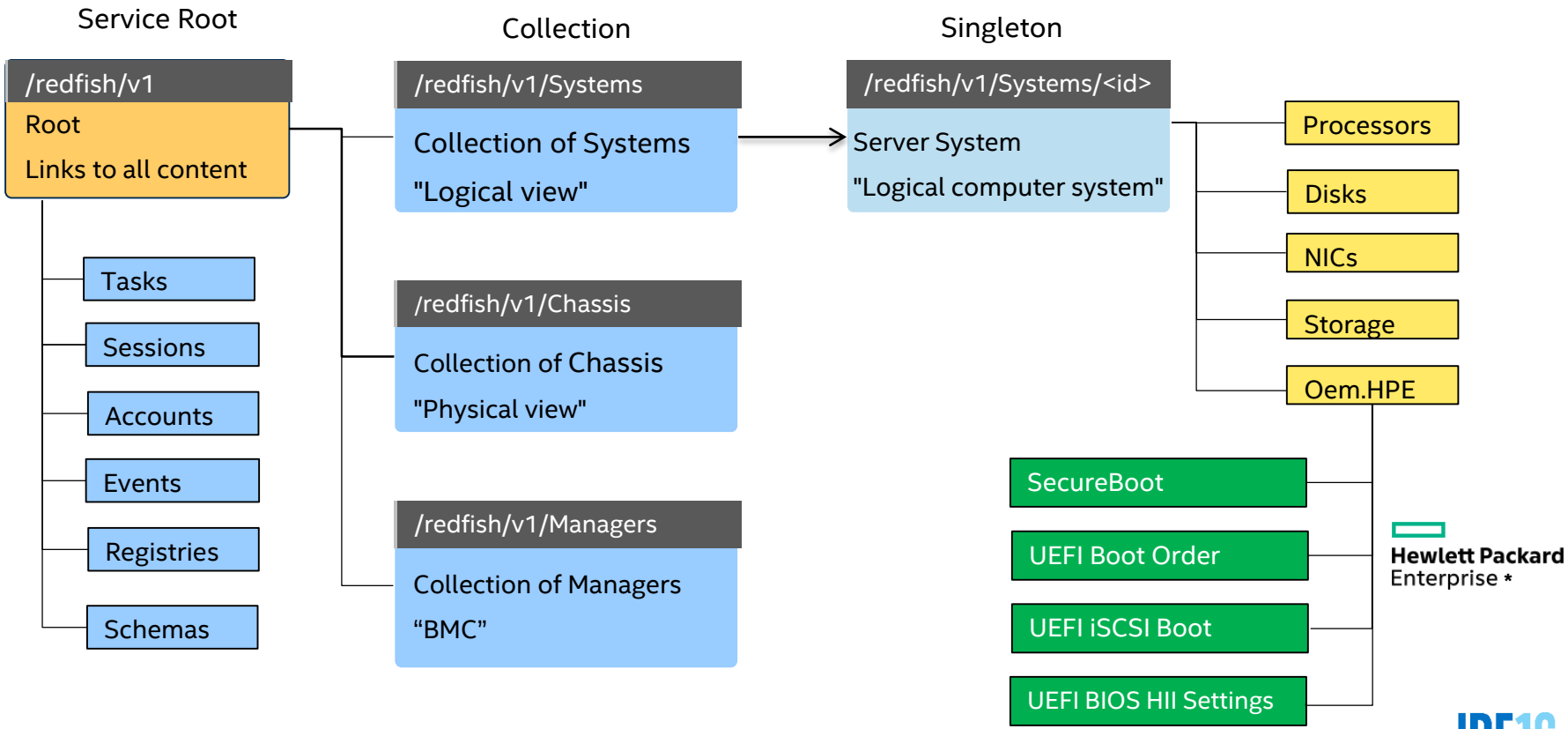
客户端 Python* 代码

```
rawData = urllib.urlopen('https://192.168.0.1/redfish/v1/Systems/1')
jsonData = json.loads(rawData)
print( jsonData['SerialNumber'] )
```

输出

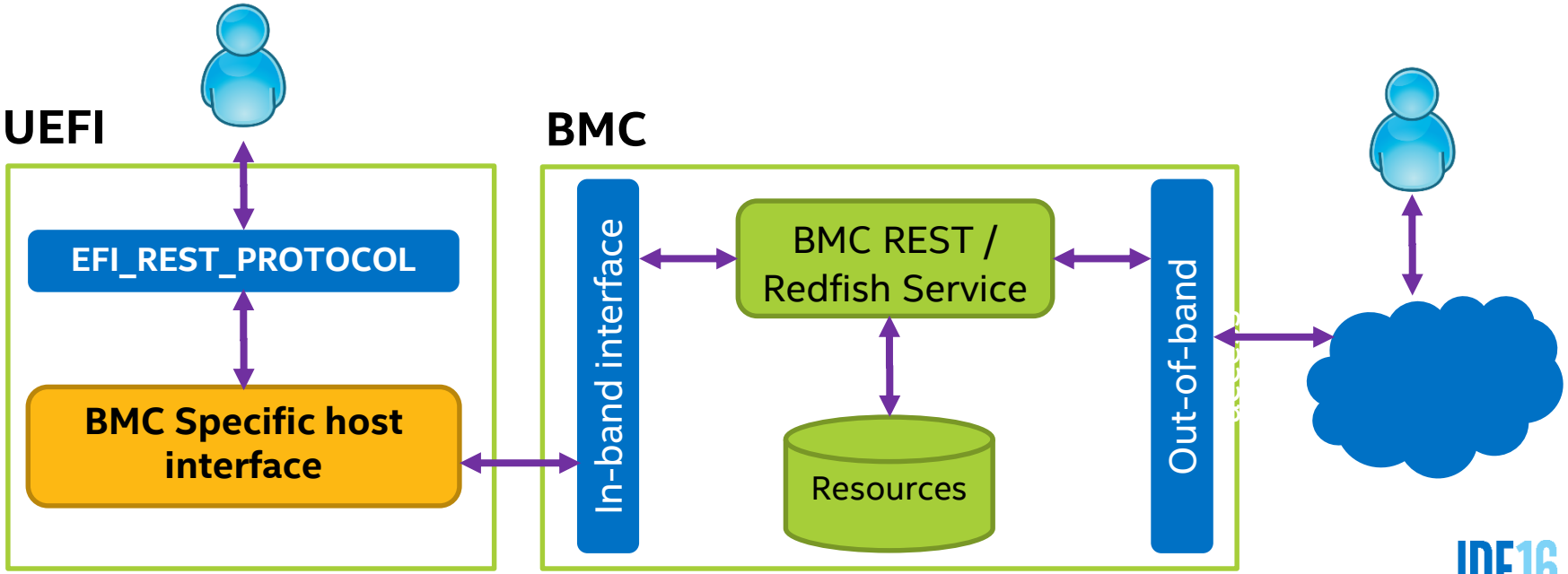
```
0AB8012GQ0
```

Redfish 资源图

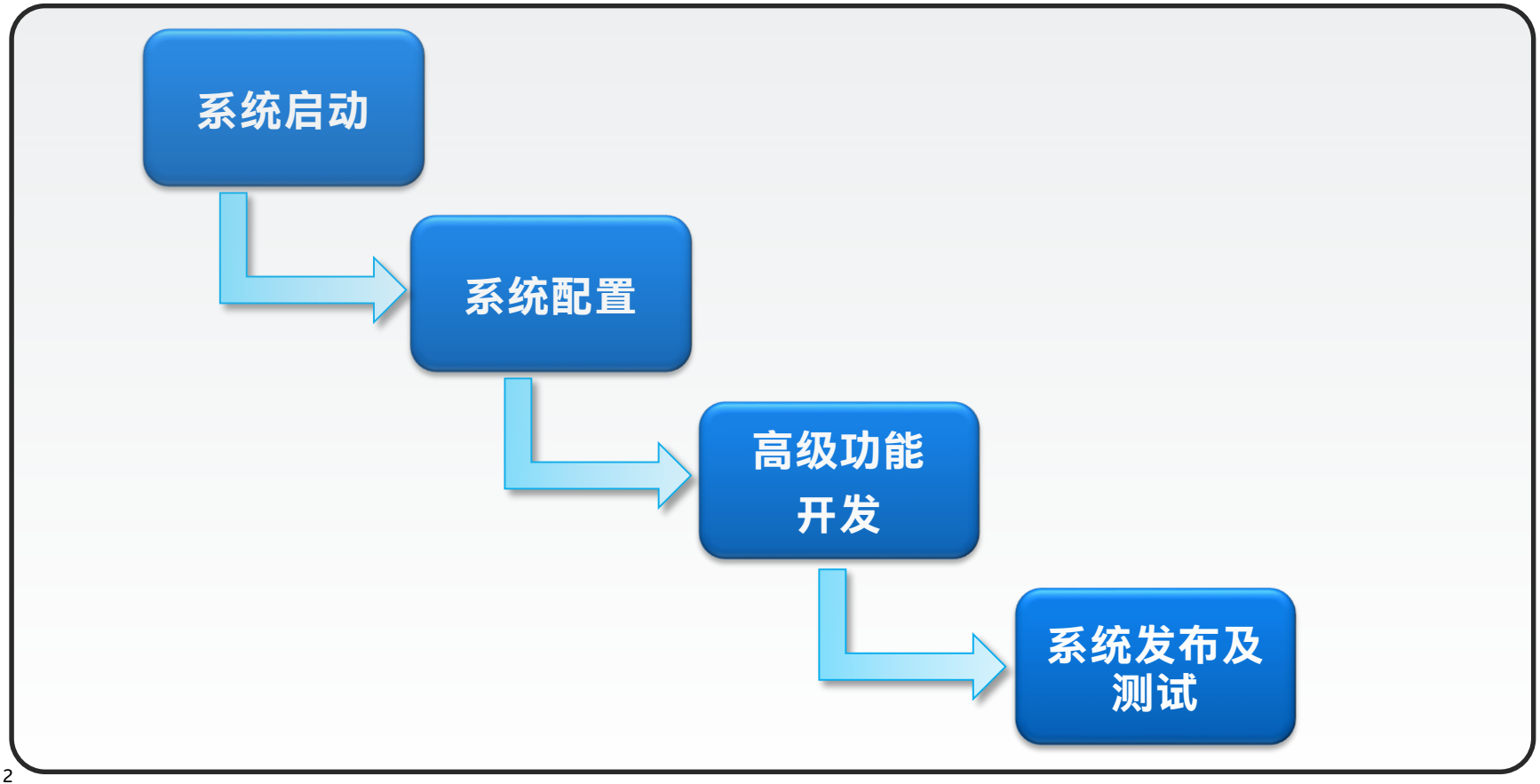


UEFI REST 协议

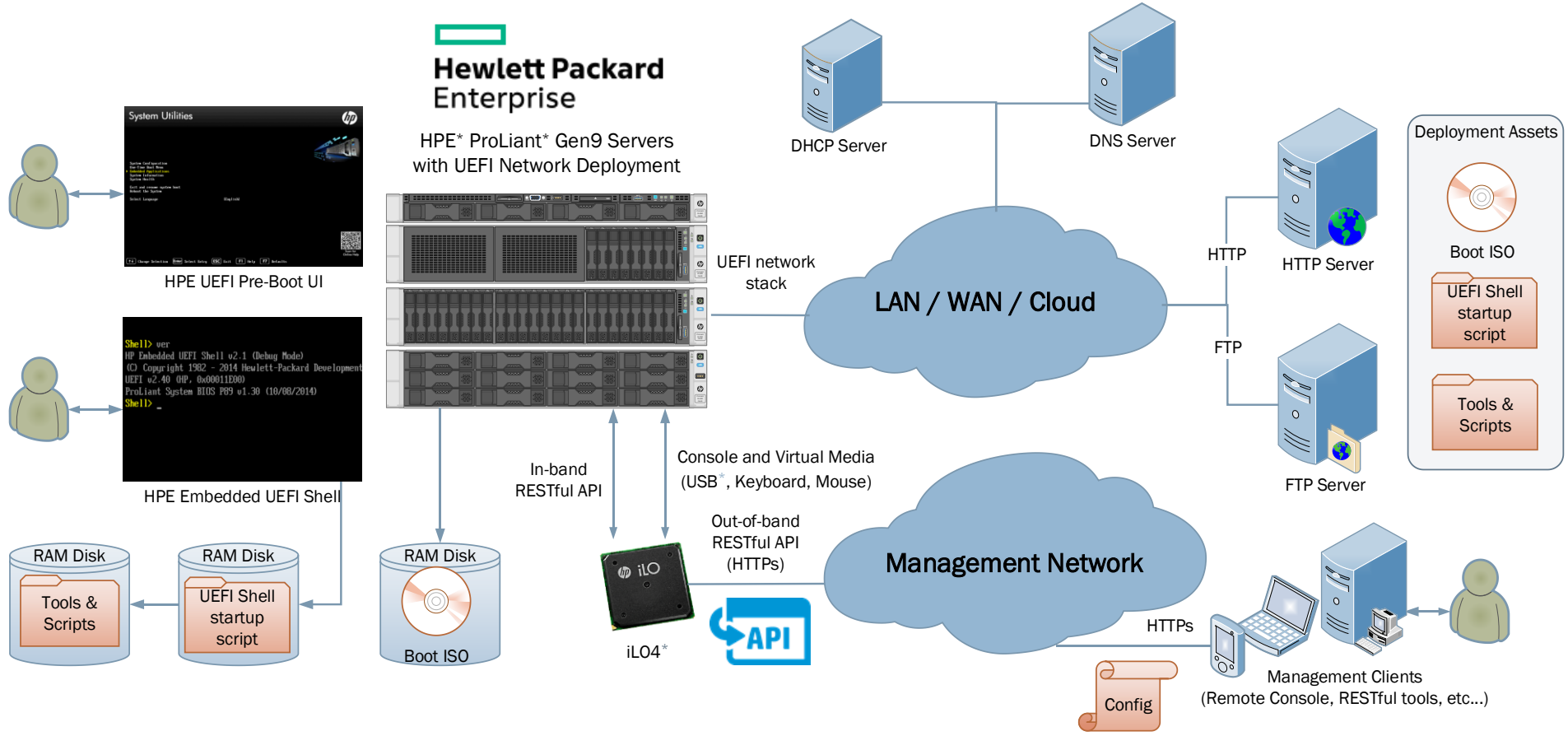
- UEFI 2.5规范定义
- 预启动环境下，支持带内访问RESTful接口(如Redfish)的标准协议
- 将BMC各种(厂商特有的)访问方式抽象化



UEFI 固件开发流程



UEFI在HPE* 服务器上的部署方案



HPE* Redfish范例: UEFI安全启动

GET @
/redfish/v1/systems/1/secureboot

- 开启/禁用UEFI安全启动
- 重置所有UEFI安全启动相关的UEFI变量
- 清空所有密钥 (退回到设置模式)


```
{
    "Name": "SecureBoot",
    "ResetAllKeys": false,
    "ResetToDefaultKeys": false,
    "SecureBootCurrentState": false,
    "SecureBootEnable": false,
    "Type": "HpSecureBoot.0.9.5"
}
```

HPE* Redfish范例: UEFI BIOS HII 配置

GET @ /redfish/v1/systems/1/bios

- 包含所有UEFI BIOS的HII配置信息(名称/值)
- HII meta-data记录在属性注册表中
- 通过名称/值来查找属性注册表中的meta-data


```
"AdminName": "",
"AdminOtherInfo": "",
"AdminPassword": null,
"AdminPhone": "5555555",
"AdvancedMemProtection": "AdvancedEcc",
"AsrStatus": "Enabled",
"AsrTimeoutMinutes": "10",
"AssetTagProtection": "Unlocked",
"AttributeRegistry": "HpBiosAttributeRegistryP89.1.0.40",
"AutoPowerOn": "RestoreLastState",
"BootMode": "Uefi",
```

HPE* Redfish范例: UEFI BIOS HII 配置

GET @ /redfish/v1/registries/HpBiosAttributeRegistryP89.1.0.40


```
{
    "AttributeName": "BootMode",
    "DisplayName": "Boot Mode",
    "HelpText": "Use this option to select the boot mode of the system. Se
    "WarningText": "Boot Mode changes require a system reboot in order to
    "ReadOnly": false,
    "GrayOut": false,
    "Type": "Enumeration",
    "MenuPath": "./BootOptions",
    "DisplayOrder": 81,
    "CurrentValue": null,
    "Value": [
        {
            "ValueName": "Uefi",
            "ValueDisplayName": "UEFI Mode"
        },
        {
            "ValueName": "LegacyBios",
            "ValueDisplayName": "Legacy BIOS Mode"
        }
    ]
},
```

UEFI Shell启动脚本范例

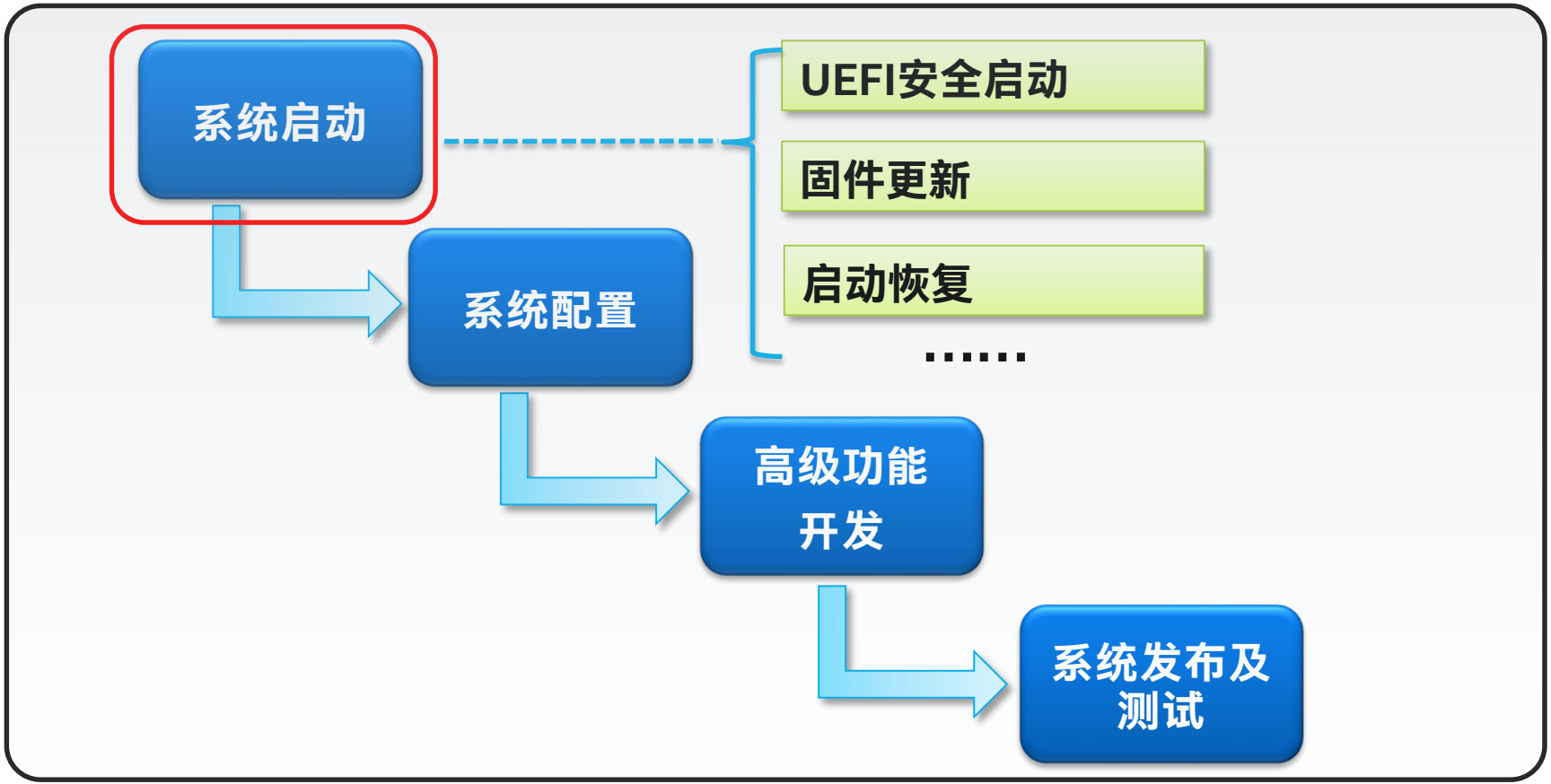
```
# Create FAT32 RAM Disk
ramdisk -c -s 512 -v MYRAMDISK -t F32
FS0:


# Download provisioning OS files from HTTP to RAM Disk
webclient -g http://repo.hpe.com/deploy/efilinux.efi
webclient -g http://repo.hpe.com/deploy/deploy.kernel
webclient -g http://repo.hpe.com/deploy/deploy.ramdisk


# Start provisioning OS
efilinux.efi -f deploy.kernel initrd=deploy.ramdisk
```

应用UEFI高级功能从而加快固件开发的实用范例

议程

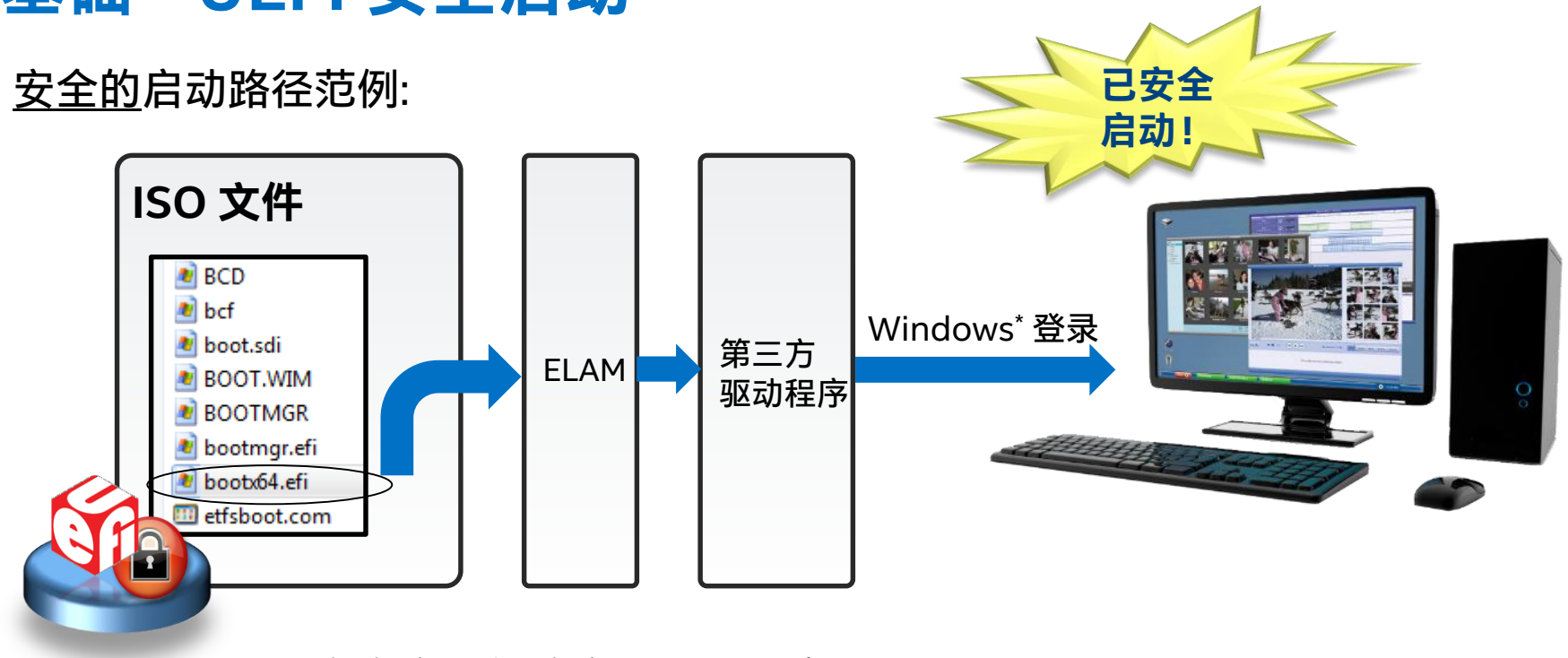
- UEFI和ACPI技术规范的最新信息
- Redfish RESTful技术在数据中心的应用范例
- UEFI核心功能应用于UEFI开发
- 总结

用UEFI核心功能进行开发



基础 - UEFI 安全启动

安全的启动路径范例:



- UEFI安全启动保护启动引导程序 (bootx64.efi)
- 启动引导程序保护ELAM (早期加载的反恶意软件)
- 木马软件无法避开反恶意软件的检查

升级 – 可定制的UEFI安全启动

部署

基础	升级
平台特有的 PK_{pub} 清除方案	增加定制安全启动密钥的 标准化方案
设置模式 用户模式	设置模式　用户模式 审计模式 已部署模式

优势

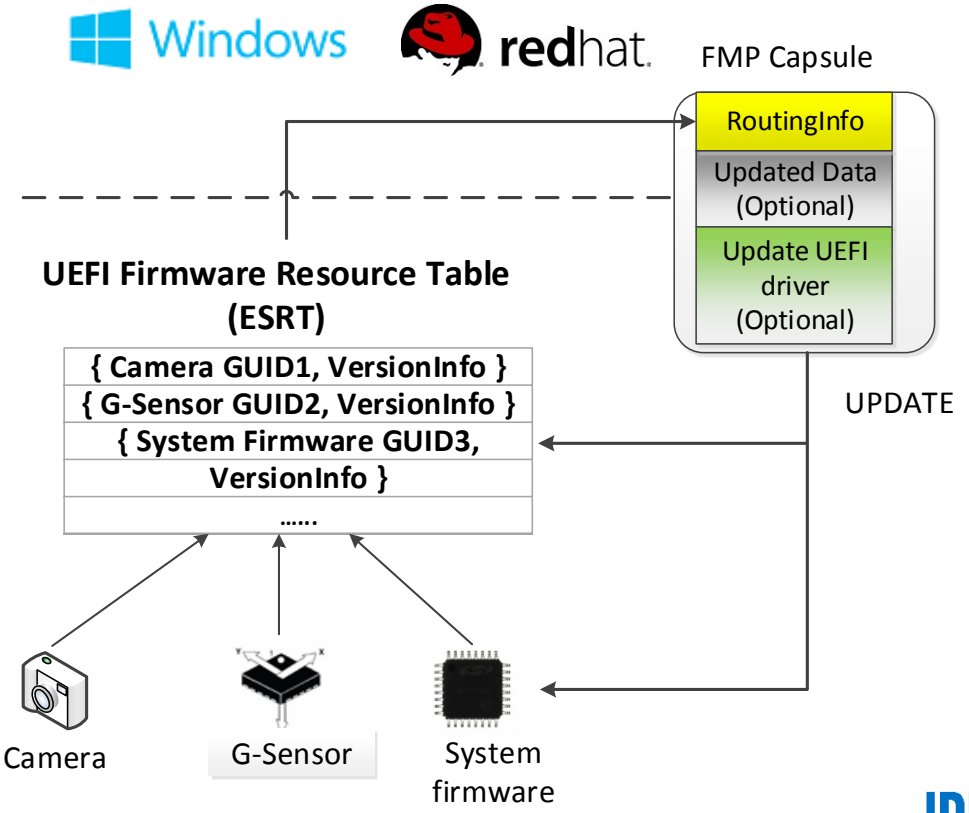
- 不含特有解决方案 → 安全性
- 提高利用率 → 灵活性
- 保存查证结果 → 可扩展性

可定制的UEFI安全启动进一步降低平台特有方案引入的安全风险。目前处于和OS供应商合作以提高互操作性和接受度的推广阶段。

固件安全升级

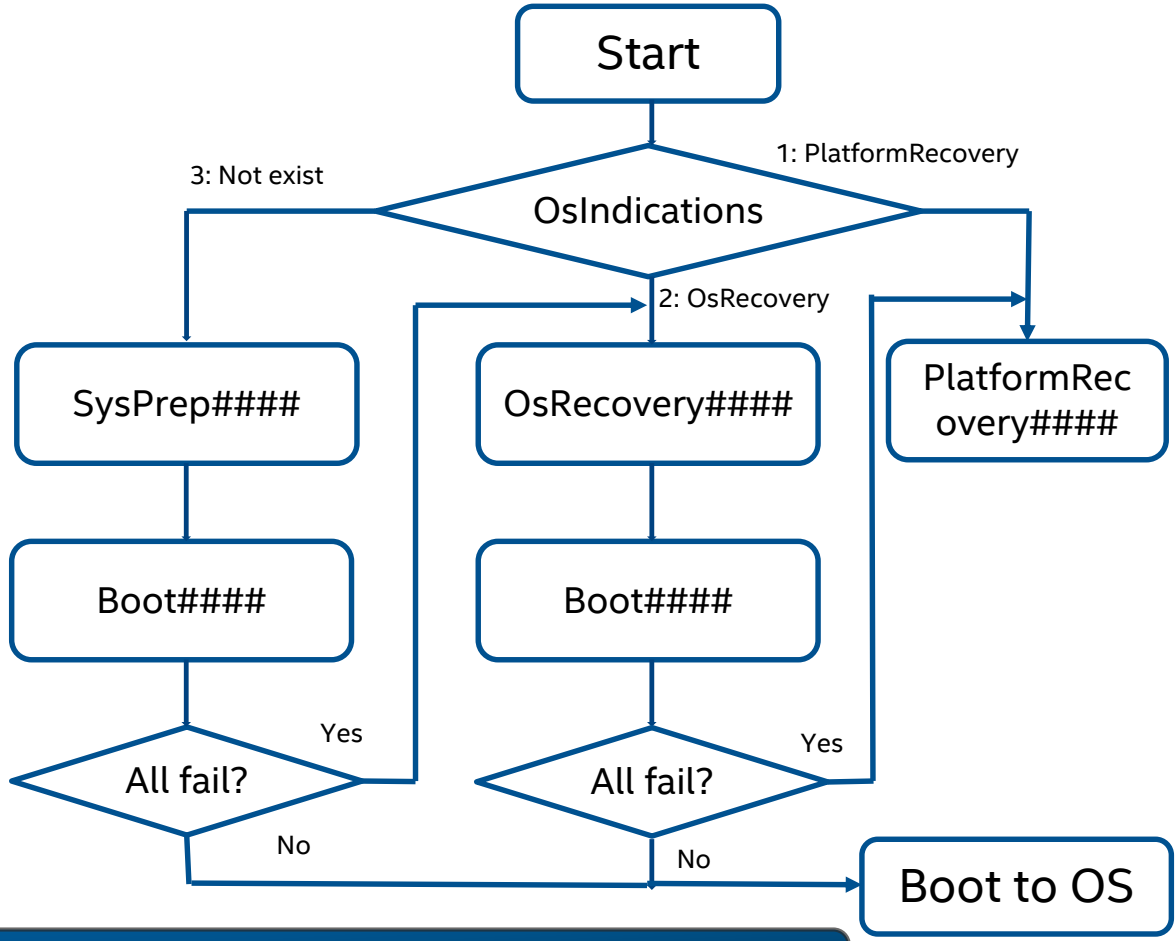
- 固件升级中的双重保护:
  - OS在构建capsule时验证升级驱动程序
  - 在执行升级前UEFI安全启动验证capsule中有效负载数据

- 相关技术:
  - ESRT
  - FMPv3
  - FMP capsule



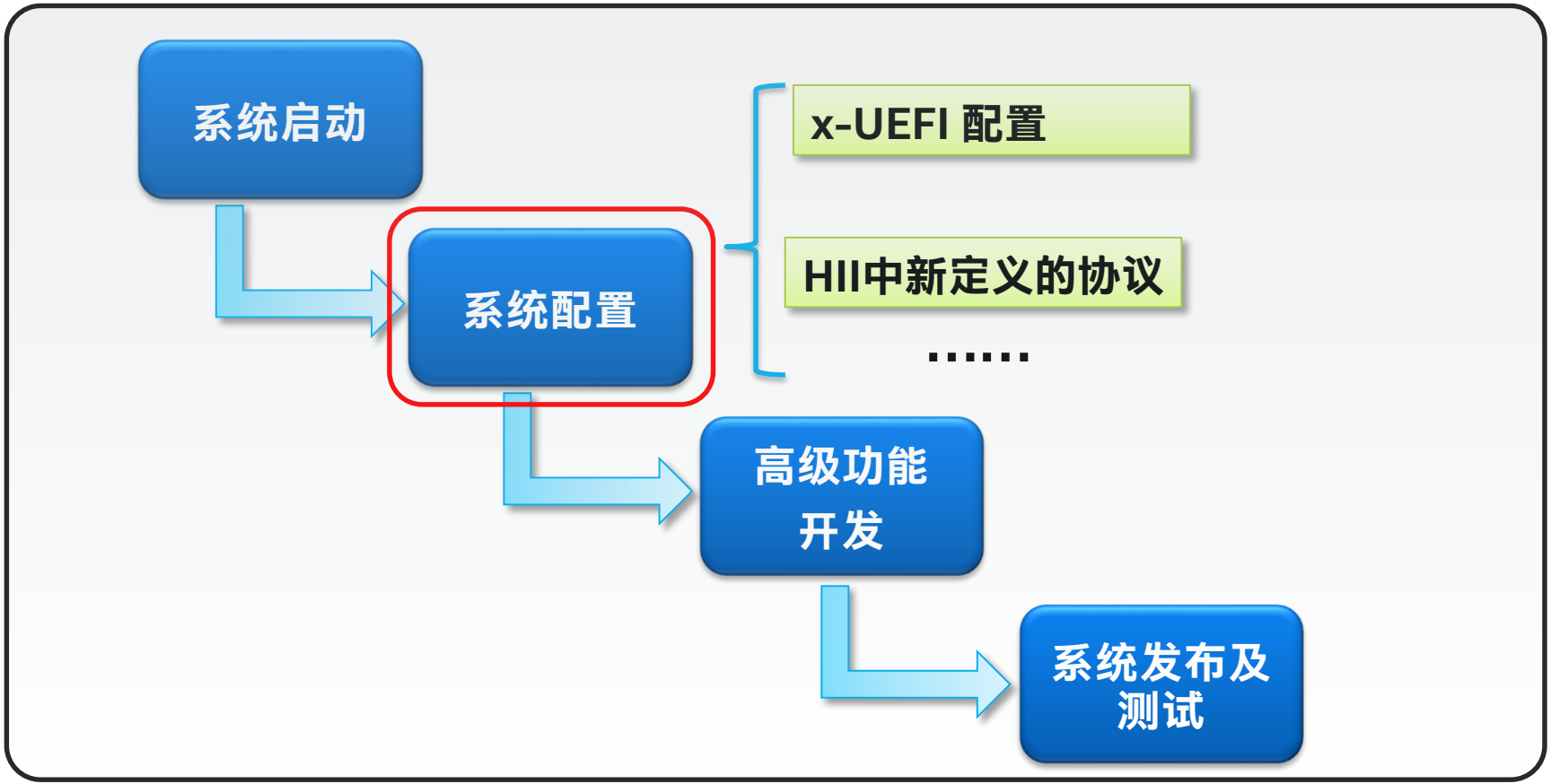
启动恢复

- 相关技术
  - OS定义的恢复策略
  - 平台定义的恢复策略
  - 恢复策略使用认证技术进行保护，相关UEFI变量如下:
    - OsRecoveryOrder
    - dbrDefault, dbr
  - 支持缺省平台恢复机制



安全技术升级在系统启动阶段加速固件安全性开发

用UEFI核心功能进行开发



x-UEFI 脚本化配置

- 基于不同命名空间中的关键词
- 利用现有的UEFI HII架构

- 技术要点:
  - x-UEFI 语言
  - Keyword Handler 协议

x-UEFI 配置范例

iSCSIInitiatorName

VFR file

```
string  varid    = ISCSI_CONFIG_IFR_NVDATA.InitiatorName,
          prompt  = STRING_TOKEN(STR_ISCSI_CONFIG_INIT_NAME),
```

UNI file

```
#string STR_ISCSI_CONFIG_INIT_NAME    #language en-US "iSCSI Initiator Name"
#string STR_ISCSI_CONFIG_INIT_NAME    #language x-UEFI "iSCSIInitiatorName"
```

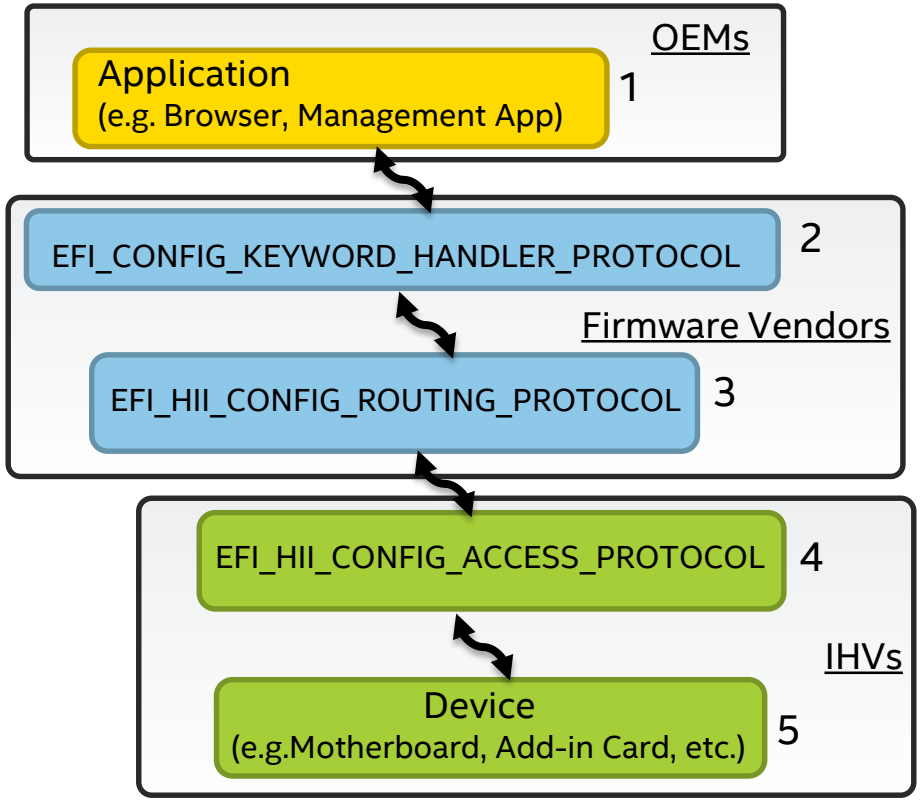
Script file

```
IScsiScript -i iqn.edkii.intel.com
```

x-UEFI配置如何实现?

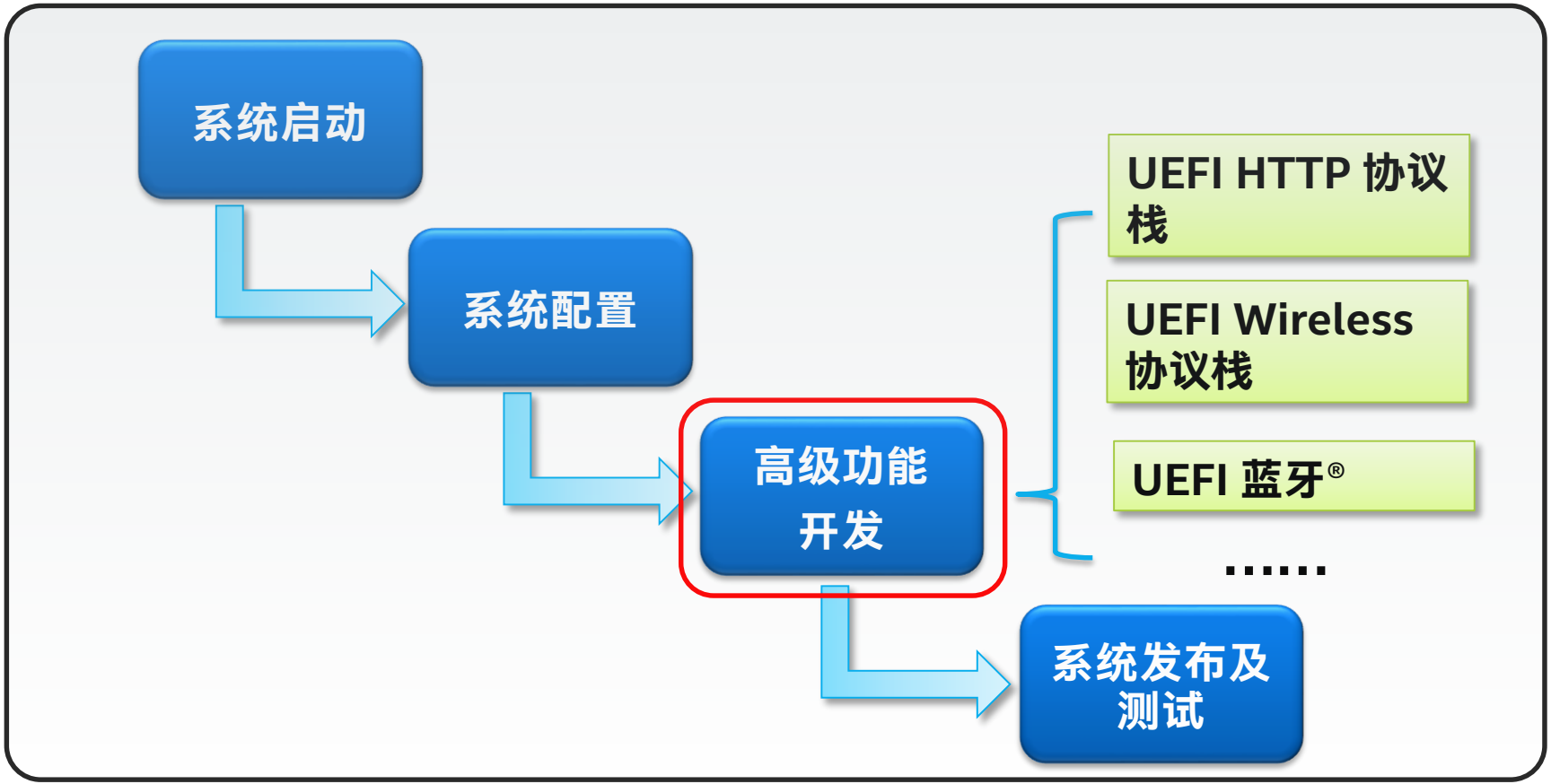
- OEMs …
  - 查阅关键词

    http://www.uefi.org/configNamespace
  - 调用 KeywordHandler.GetData/SetData
- Firmware Vendors …
  - 从英特尔® UEFI 开发套件 (Intel® UDK) 2015获取HII最新实现
- IHVs …
  - 定义并注册x-UEFI关键词
  - 在ConfigAccess.RouteConfig 中实现基于关键词的配置



配置技术升级在系统配置阶段 加速固件开发

用UEFI核心功能进行开发

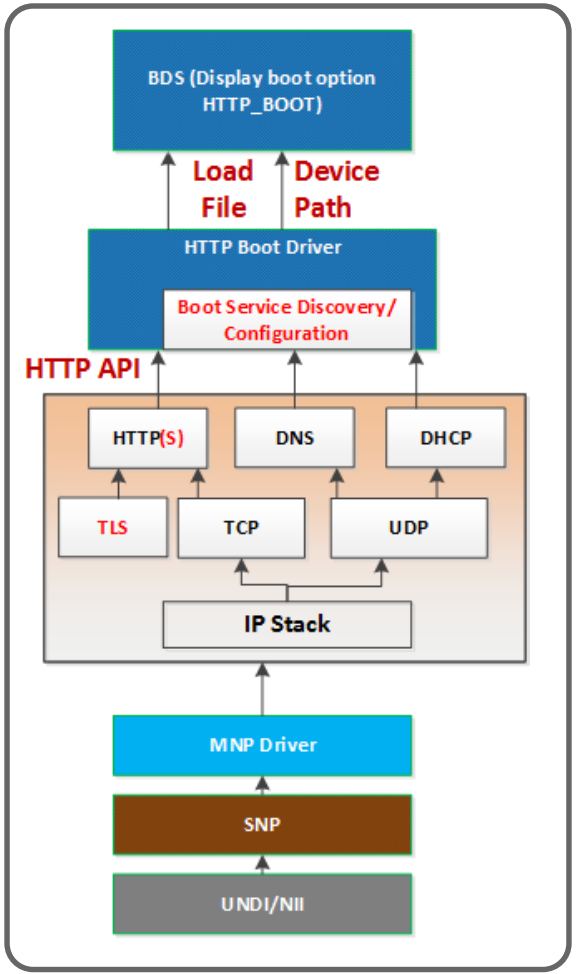


UEFI HTTP 协议栈

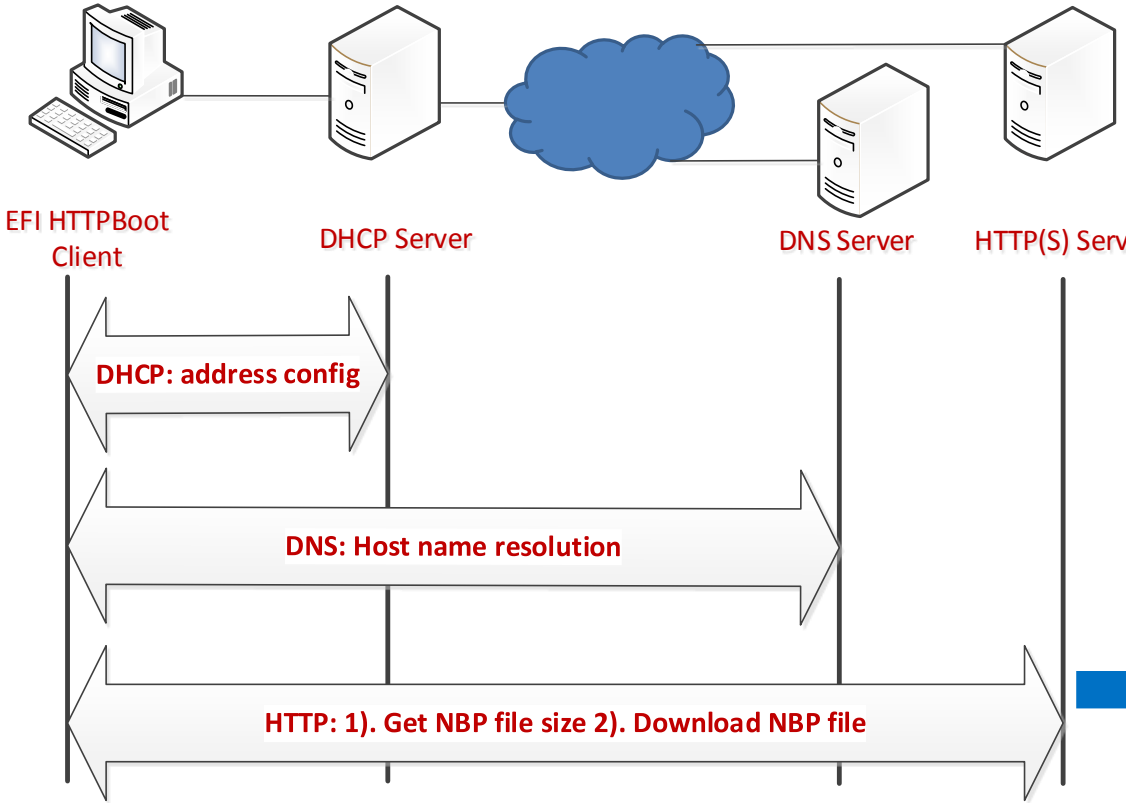
新模块

驱动程序	库
HTTP启动程序 HTTP 程序 HTTP 工具程序 TLS 程序	HTTP 库 TlsLib库 OpenslTlsLib库

- 灵活的网络部署方案
- 对家庭环境的支持
- 对企业环境的支持



HTTP(S) 启动流程



启动成功！

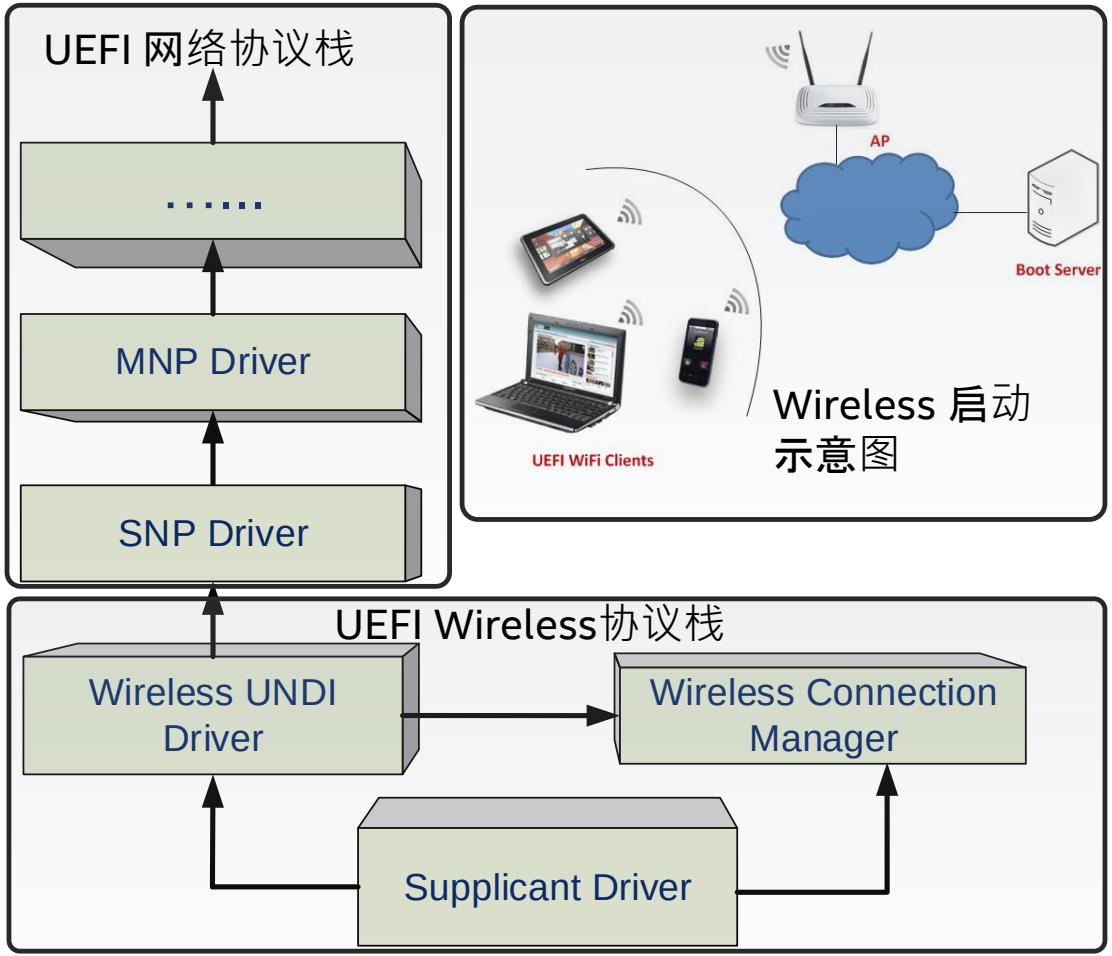
演示 - UEFI HTTP(S) 启动

- 步骤 0: 配置TLS证书
  - 用于HTTPS启动
- 步骤 1: 配置启动URI
  - 进入设备管理
  - 选择一张网卡
  - 进入HTTP启动配置
  - 输入启动URI并保存
- 步骤 2: 找到启动选项
  - 进入启动管理
  - 选择新增加的启动选项
- 步骤 3: 启动Windows* 预安装环境

TLS仅是一个补丁程序。目前的实现中对证书的管理仍然不够安全。希望和业界合作以加强安全性以及和OS供应商合作增加互操作性。

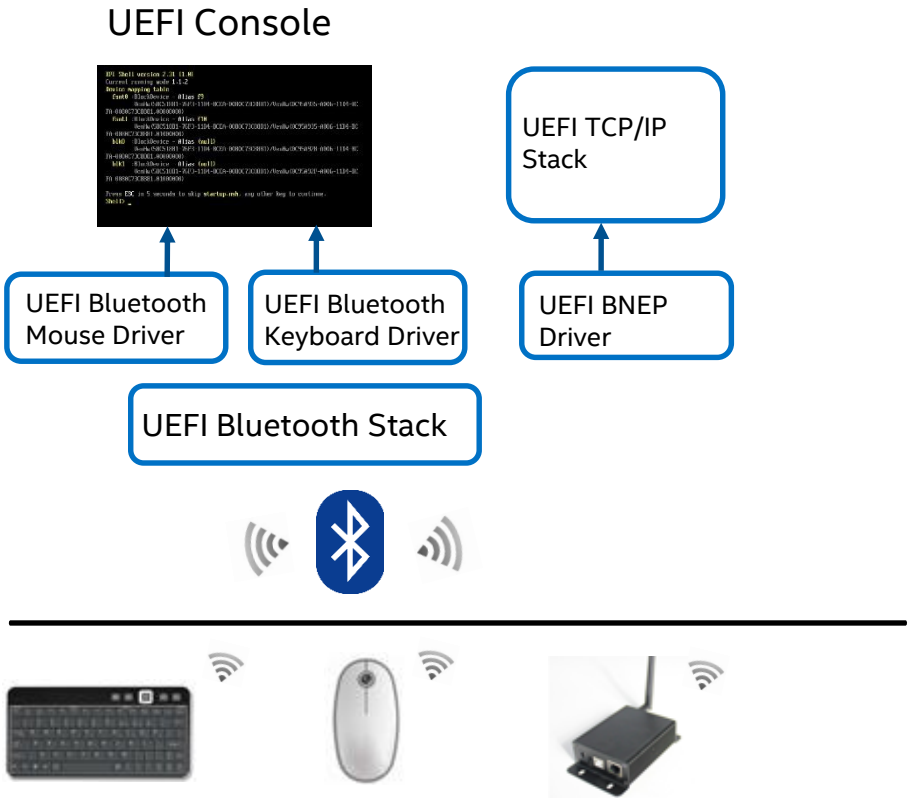
UEFI Wireless 协议栈

- 符合802.11协议规范的无线协议栈:
  - 基于HII的连接管理
  - 提供通用的supplicant 功能，包括:
    - PSK 认证
    - EAP 802.1x 认证
  - CCMP 加密



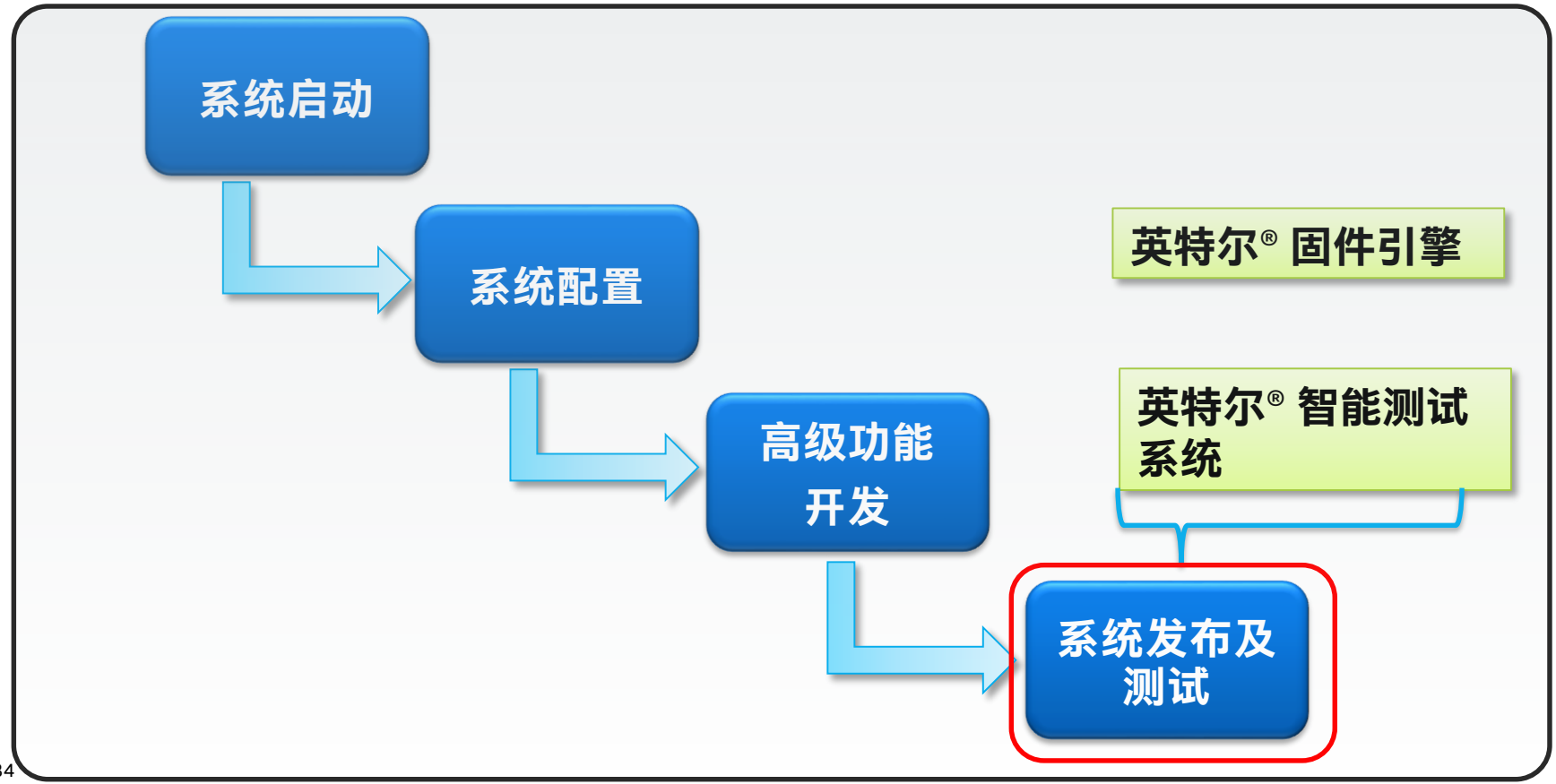
UEFI 蓝牙®

- 提供通用 I/O 接口:
  - UEFI 设备驱动程序可提供丰富的功能
- UEFI 蓝牙® 协议层包括:
  - 蓝牙®主控制器
  - 蓝牙®总线
  - 蓝牙®服务



连接技术升级在高级功能开发阶段加速固件开发

将UEFI核心功能应用于UEFI开发



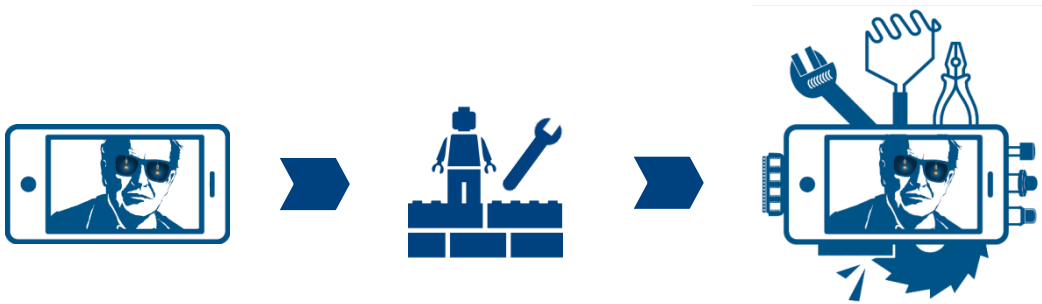
英特尔® 固件引擎

无需源代码即可为IoT设备快速生成固件

可扩展的二进制固件架构

基于已验证参考设计的二次开发

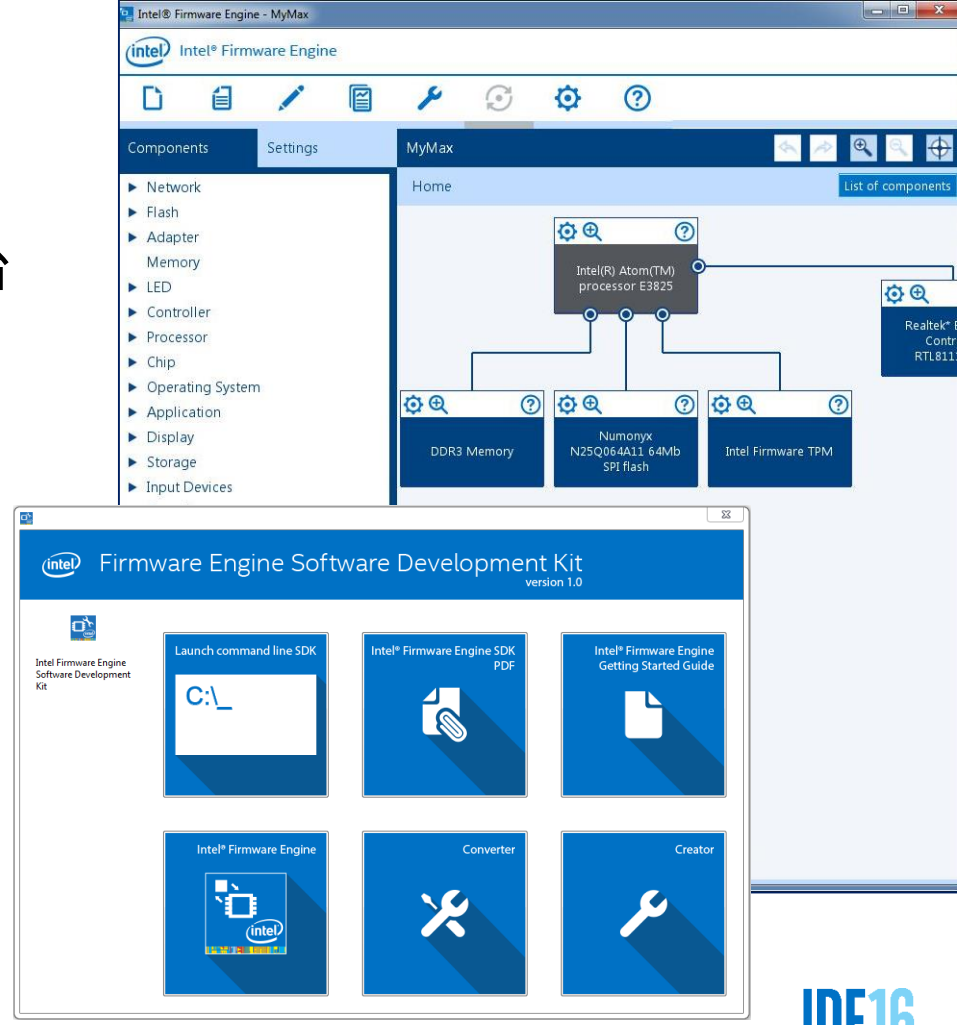
GUI开发进一步缩短上市时间



更多信息：
intel.com/firmwareengine

英特尔® 固件引擎

- 应用程序、SDK以及开放式硬件平台在这里提供下载：
  intel.com/firmwareengine
- 英特尔® 固件引擎2.0已发布
- SDK新版本将于2016年四月份发布
- 将支持更多英特尔IoT平台



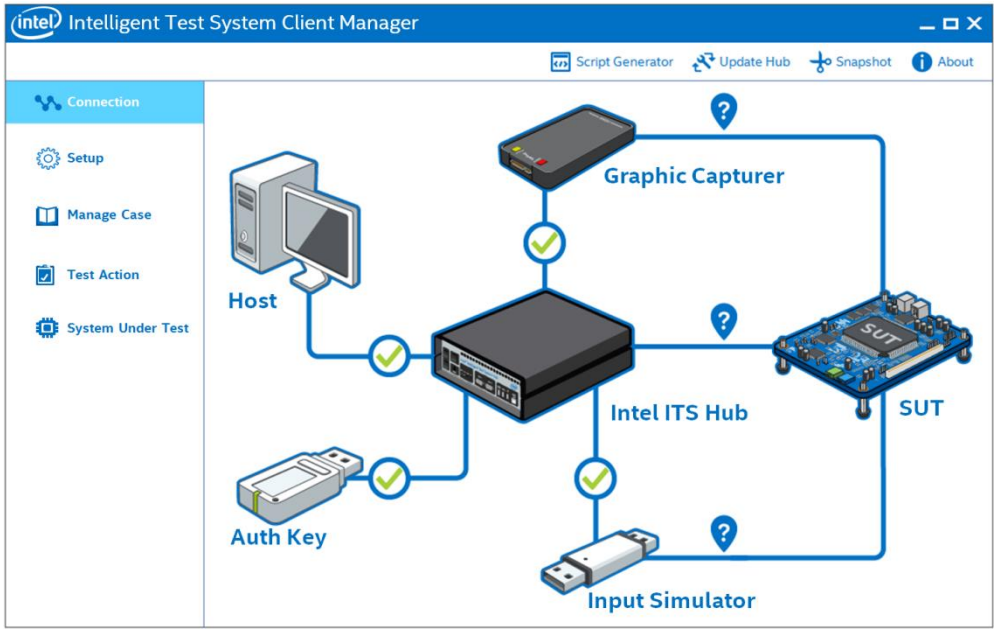
英特尔® 智能测试系统 (英特尔® ITS)

可扩展的硬件/软件测试框架

自动测试、设备控制以及UEFI代码覆盖率检查

减少成本同时提高测试效率

英特尔® 固件引擎和英特尔® 智能测试系统简化固件发布和固件测试流程



更多信息: intel.com/intel-its

议程

- UEFI和ACPI技术规范的最新信息
- Redfish RESTful技术在数据中心的应用范例
- UEFI核心功能应用于UEFI开发
- 总结

总结和下一步计划

- UEFI和ACPI规范的更新有助于加速固件开发
- UEFI高级功能加速了固件开发进程，帮助了Redfish在数据中心中使用 RESTful管理模式
- 更多在安全、配置、网络相关方面的升级已准备就绪
- 英特尔® 固件引擎和英特尔® 智能测试系统极大地简化了固件发布和固件测试流程

下一步计划:

- 在固件开发中使用UEFI 2.6实现的高级功能
- 在服务器和管理软件上使用Redfish
- 进一步加强业界合作，提升UEFI高级功能的安全性、互操作性以及接受度

补充信息

- 您可通过IDF网站的技术课程目录下载此次课程的PDF演讲文稿 www.intel.com/idfsessionsSZ 也可以在技术课程目录的首页链接下载。

- 更多相关信息：
  - 英特尔® 固件资源中心: firmware.intel.com
  - UEFI 论坛学习中心: uefi.org/learning_center
  - UEFI 和ACPI 协议规范: www.uefi.org/specs/
  - Redfish 协议规范: www.dmtf.org/standards/redfish

英特尔EDK II和UEFI 开发人员调查

英特尔正在开展一项EDKII和UEFI开发工具相关的调查。我们希望得知您常用的编译器、调试方法、以及在固件开发方面我们仍需提升的地方。

请访问以下链接或扫二维码参与：

http://intelcustomer.az1.qualtrics.com/SE/?SID=SV_6lJbxG5BYFFMPSl&Source=IDF

其他技术课程

课程编号	标题	日期	时间	教室
STTS001 ✓	使用 UEFI 高级功能加速固件开发	周三	13:15	演播厅
STTS002	借助面向 WebRTC 的英特尔®协同通信开发套件增强互联网上的实时通信用户体验	周三	14:30	演播厅
STTS003	规划和预测大数据与物联网解决方案	周三	15:45	演播厅

✓ = 完毕

下一个精彩是什么?

Legal Notices and Disclaimers

Do not translate

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure.

Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

Statements in this document that refer to Intel's plans and expectations for the quarter, the year, and the future, are forward-looking statements that involve a number of risks and uncertainties. A detailed discussion of the factors that could affect Intel's results and plans is included in Intel's SEC filings, including the annual report on Form 10-K.

The products described 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.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

Intel, 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.

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Intel is under license.

Risk Factors

Do not translate

The above statements and any others in this document that refer to future plans and expectations are forward-looking statements that involve a number of risks and uncertainties. Words such as "anticipates," "expects," "intends," "goals," "plans," "believes," "seeks," "estimates," "continues," "may," "will," "should," and variations of such words and similar expressions are intended to identify such 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 could differ from expectations due to factors including changes in business and economic conditions; consumer confidence or income levels; the introduction, availability and market acceptance of Intel's products, products used together with Intel products 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'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. Results may also be affected by the formal or informal imposition by countries of new or revised export and/or import and doing-business regulations, which could be changed without prior notice. Intel operates in highly competitive industries and its operations have high costs that are either fixed or difficult to reduce in the short term. The amount, timing and execution of Intel's stock repurchase program could be affected by changes in Intel's priorities for the use of cash, such as operational spending, capital spending, acquisitions, and as a result of changes to Intel's cash flows or changes in tax laws. Product defects or errata (deviations from published specifications) may adversely impact our expenses, revenues and reputation. Intel's results could be affected by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust, disclosure and other issues. 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. Intel's results may be affected by the timing of closing of acquisitions, divestitures and other significant transactions. We completed our acquisition of Altera on December 28, 2015 and risks associated with that acquisition are described in the “Forward Looking Statements” paragraph of Intel’s press release dated June 1, 2015, which risk factors are incorporated by reference herein. 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. 1/14/16

补充

UEFI Shell 2.2 规范更新

- 网络相关的更新
- 允许调用**Execute()** 时不重新嵌套新的shell
- 增加自动退出的命令行参数
- **setvar**命令重构
- 以下命令引入新功能

  dh, disconnect, comp, dmem, cls, reset, pci, bcfg, dmpstore

PI Packaging 1.1 的更新

- 基于离散型子集配置模式传递PCD配置信息
- 本地化发布包中的名字
- 传递详细的有关协议/PPI/GUIDs的生成信息
- 传递二进制模块中PCD的使用方法
- 传递详细的有关协议/PPI/GUIDs的使用信息
- 传递PCD显示信息
- 传递PCD枚举类信息(允许字符串)
- 支持抽象化类型
- 传递BY_START/TO_START相互作用信息
- 传递产品中有关协议/PPI/GUIDs的设置或生成的受限信息

使用HPREST的配置脚本范例

```
# Login to iLO
hprest login https://clientilo.domain.com -u username -p password

# Configure UEFI network settings (Use Auto and DHCP defaults)
hprest set PreBootNetwork=Auto --selector HpBios.
hprest set Dhcpv4=Enabled

# Configure UEFI Shell startup script from URL
hprest set UefiShellStartup=Enabled
hprest set UefiShellStartupLocation=NetworkLocation
hprest set UefiShellStartupUrl=http://192.168.1.1/deploy/startup.nsh

# Set one-time-boot to Embedded UEFI Shell
hprest set Boot/BootSourceOverrideEnabled=Once --selector ComputerSystem.
hprest set Boot/BootSourceOverrideTarget=UefiShell

# Save and reboot server
hprest commit --reboot=ON
```