



# **Using a BIOS to unleash the power of the VIA chipset for Digital Home Applications**

Steve Dearden  
General Software

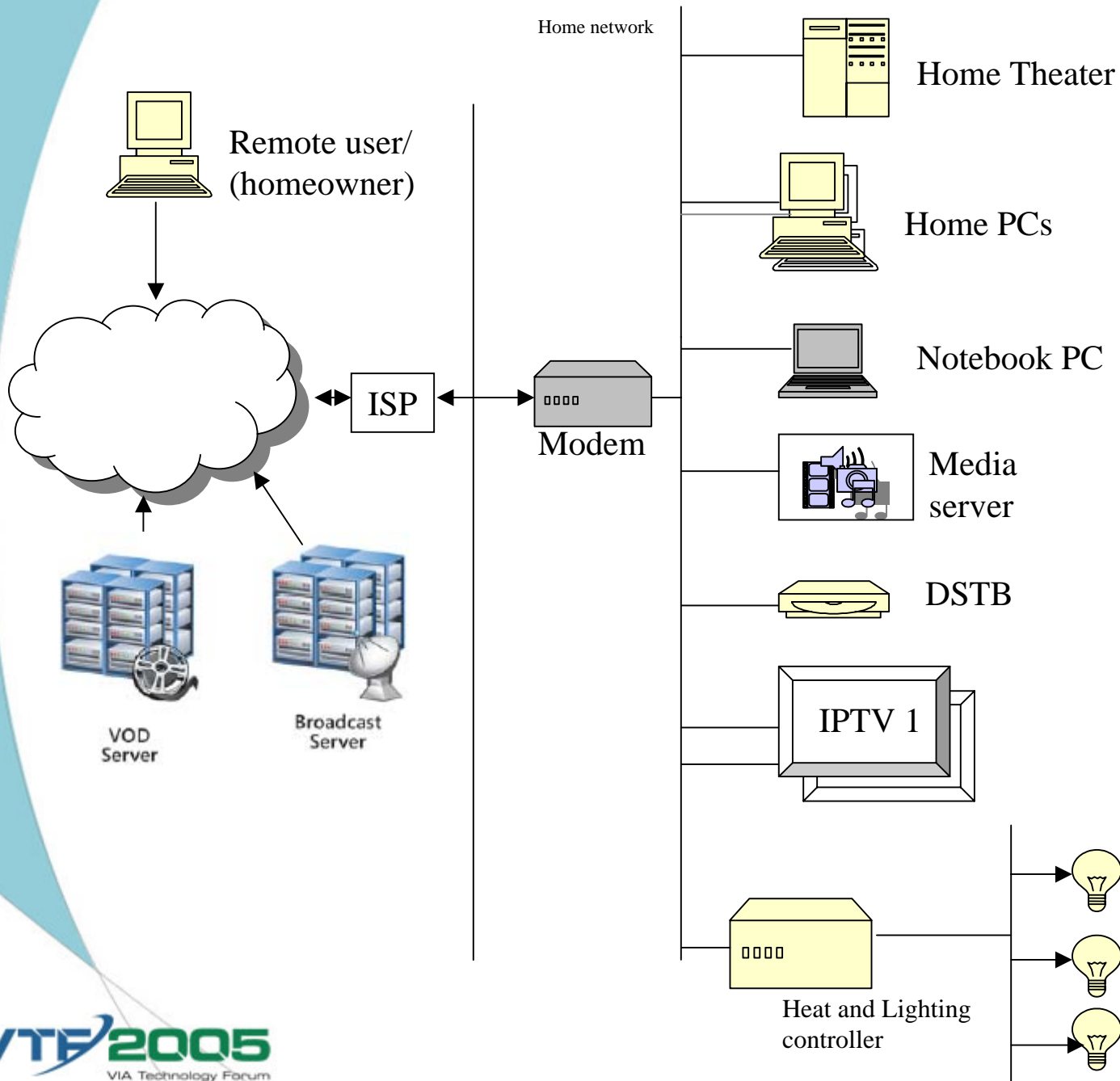
Enabling  
Digital Brilliance

# Agenda

- Introduction
- Understanding Digital Home platform requirements
- Unleashing the power of the VIA chipset
- Conclusion

# Digital Home – an Introduction

- Integrated digital technologies for entertainment, communication and control
- Combination of:
  - Desktop & notebook PCs
  - PDAs
  - Multimedia devices, DSTBs, entertainment
  - Wired and wireless networking
  - Environmental controls



# Digital Home – Challenging new Requirements

- New demands, e.g.:
  - 'Instant On' appliances
  - Remote updates
  - Security
- Developers must understand:
  - New requirements
  - Technologies available for meeting them

# Objective of Presentation

- To share a view of these requirements derived from customer requests
- To discuss how they may be met using BIOS technologies on the VIA chipsets for embedded devices

# Understanding Digital Home platform requirements

- Integrating entertainment & office services introduces a slew of new requirements, including:
  - 'Instant On'
  - Security
  - Availability
  - Remote Management
  - Custom Configurations

# 'Instant On'

- Requirement:
  - Provide immediate access to primary features of device (e.g. TV tuner)
  - < 1 second from power-on to device function
- Implication:
  - Not always time for an OS to start before providing functionality

# Security

- Requirement:
  - To protect home and office data, access to Digital Home devices controlled by password
- Implication:
  - 'Who watches the consumer?' What should the user be able to do?
  - At what level should access security be controlled; the application, OS, BIOS or hardware?

# Availability

- Requirement:
  - 'Always-on' capability, or close to it, in Digital Home devices
- Implication:
  - Hardware must be designed with lowest possible COGs, without affecting reliability
  - Devices must detect and respond to software and/or hardware errors

# Remote Management

- Requirement:
  - Ability to 'push' new content (e.g. data, applications or OS) onto Digital Home device in a secure manner via network
- Implication:
  - Security concerns (e.g. unauthorized access or content upload)
  - Secure access and content authentication required

# Custom OEM Configurations

- Requirement:
  - Cheapest possible non-volatile storage for software and/or content
- Implication:
  - OEMs need to include only those firmware features required by their fixed function device

# Unleashing the power of the VIA chipset

- Above requirements cannot be achieved without help from BIOS
- BIOS level technologies and features may be harnessed to meet Digital Home device requirements

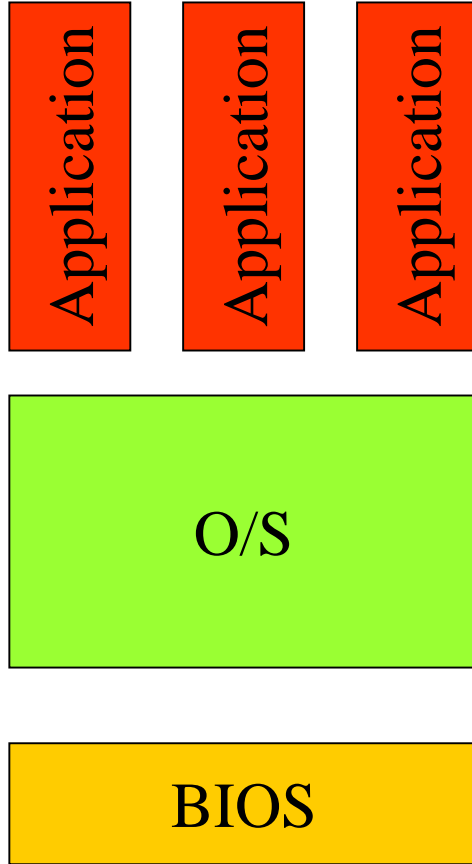
# Background - BIOS Level Technologies

- System Management Mode
  - Intended for OS independent functions
  - E.g. user interface LONG before OS loads
- Quick Boot
  - Reliable hardware does not need 30s POST
  - Simple Boot Flag spec; includes mechanism for minimizing POST & improving boot time

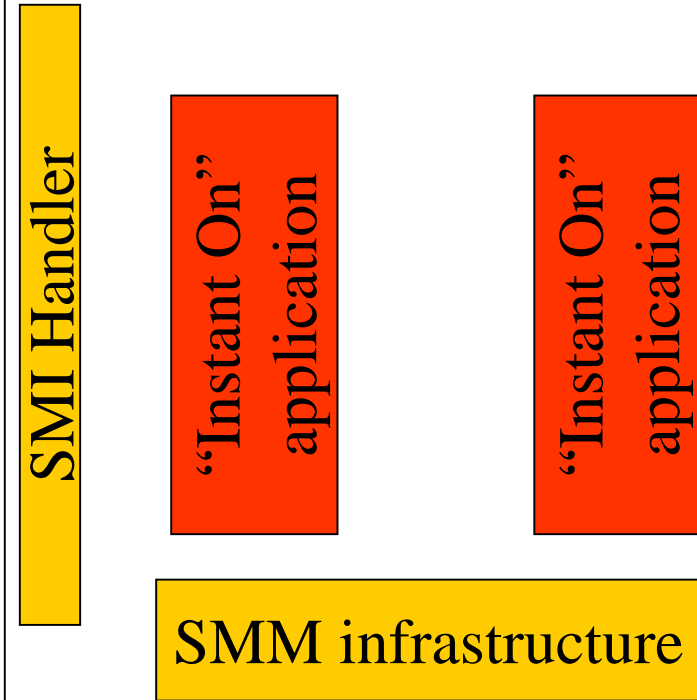
# 'Instant On'

- Quick Boot
  - Affects BIOS POST performance only
  - OS & Apps must still load and start
  - Best known performance - 4s to desktop
- SMM based interface
  - Provides best potential; power-on to SMM interface achieved in <1s
  - Provides primary interface (e.g. TV tuner) while OS & Apps load in background

## Protected Mode



## System Management Mode

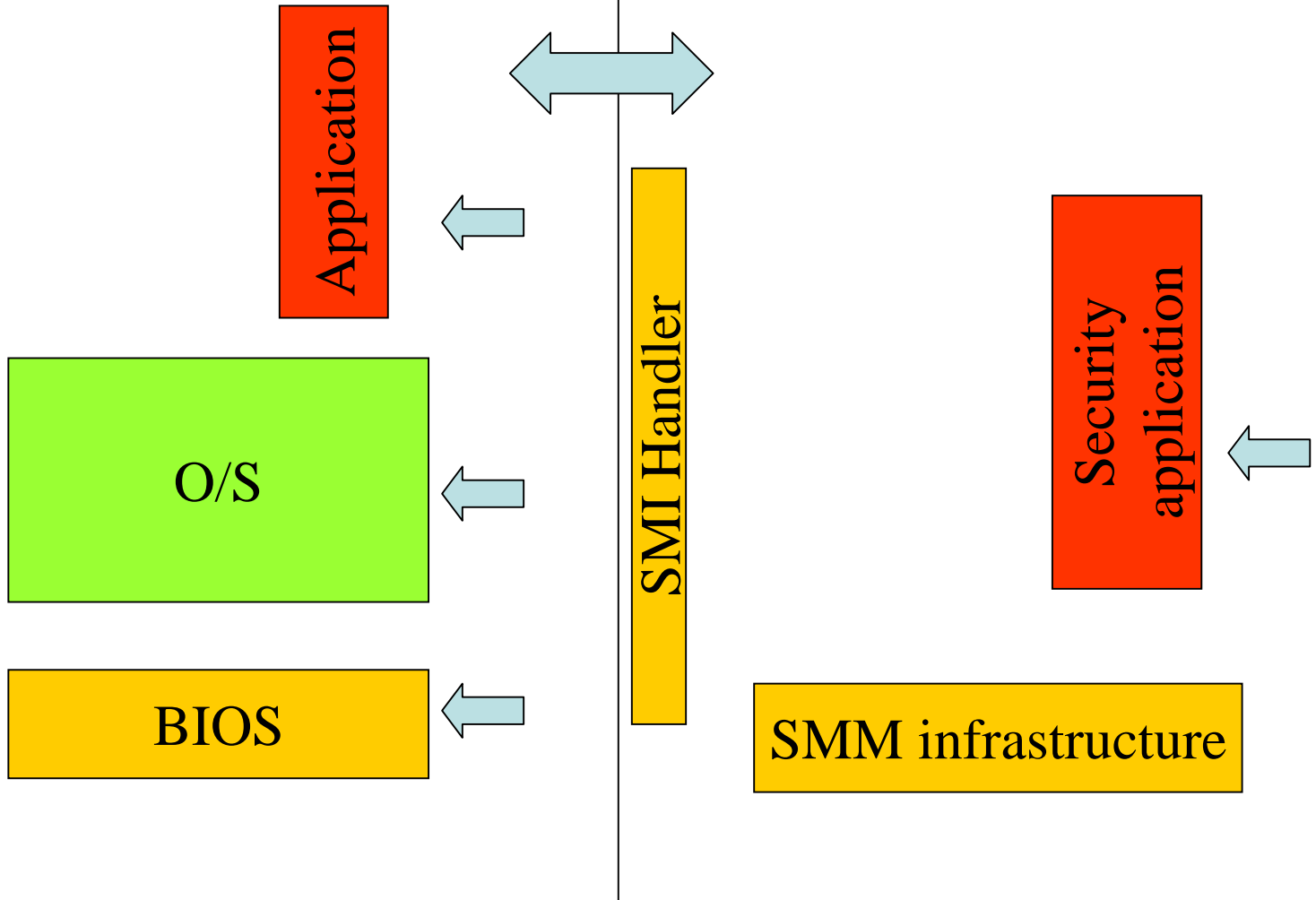


# Security

- Perfect SMM application
- Provide OS agnostic Trusted Computing Base through cryptographic challenges and responses
- Enables secure Digital Home devices from the BIOS upwards
  - Only authenticated software may be run
  - Impossible to install rogue OS

# Protected Mode

# System Management Mode



# Availability

- Perfect SMM application
- Monitor health of any OS & Apps
  - Detect BSOD, kernel panic, etc.
- Monitor health of hardware
- Respond to failures
  - Send Email
  - Restart system
  - Update system

# Protected Mode

ation

```

*** STOP: 0x0000000A (0x802aa502, 0x00000002, 0x00000000, 0xF844001C)
IRQL_NOT_LESS_OR_EQUAL*** Address fa84001c has base at fa840000 - i8042prt.SYS

CPUID: GenuineIntel 5.2.c irql:1f  SYSVER 0xF0000565

Dll Base Date Stamp - Name Dll Base Date Stamp - Name
80100000 2be154c9 - ntoskrnl.exe 80400000 2bc153b0 - hal.dll
80200000 2bd49628 - ncrcl10.sys 8025c000 2bd49688 - SCSIPTORT.SYS
80247000 2bd49683 - scsidisk.sys 802a6000 2bd496b9 - Fastfat.sys
fa800000 2bd49666 - Floppy.SYS fa810000 2bd496db - Hpps_Rec.SYS
fa820000 2bd4967e - Null.SYS fa830000 2bd4969a - Beep.SYS
fa840000 2bdaab00 - i8042prt.SYS fa850000 2bd5a020 - SERMOUSE.SYS
fa860000 2bd4966f - kbdclass.SYS fa870000 2bd49671 - MOUCLASS.SYS
fa880000 2bd49c0be - Videoprnt.SYS fa890000 2bd49638 - NCR77C22.SYS
fa0a0000 2bd4a4ce Vga.SYS fa0b0000 2bd496d0 - MofS.SYS
fa8c0000 2bd496c3 - Npfs.SYS fa8e0000 2bd496c9 - Ntfs.SYS
fa940000 2bd496df - NDIS.SYS fa930000 2bd49707 - vdlan.sys
fa970000 2bd49712 - TDI.SYS fa950000 2bd5a7fb - nbfs.sys
fa980000 2bd472406 - stream.sys fa9b0000 2bd4975f - ubah.sys
fa9c0000 2bd5b1d7 - mcsxas.sys fa9d0000 2bd4971d - netbios.sys
fa9e0000 2bd49678 - Parallel.sys fa9f0000 2bd4969f - serial.SYS
faa00000 2bd49739 - mup.sys faa40000 2bd4971f - SMBTRSUP.SYS
faa10000 2bd6f2a2 - srv.sys faa50000 2bd4971a - aft.sys
faa60000 2bd6fd80 - rdr.sys faaa0000 2bd49735 - bowser.sys

Address dword dump Build [1381] - Name
fe9cdaec fa84003c fa84003c #00000000 00000000 80149905 - i8042prt.SYS
fe9cdf8 8025dfe0 8025dfe0 ff8e6b8c 80129c2c ff8e6b94 - SCSIPTORT.SYS
fe9cdb10 8013e53a 8013e53a ff8e6b94 00000000 ff8e6b94 - ntoskrnl.exe
fe9cdb18 8010a373 8010a373 ff8e6df4 ff8e6f60 ff8e6c58 - ntoskrnl.exe
fe9c38 80105683 80105683 ff8e6f60 ff8e6c3c 8015ac7e - ntoskrnl.exe
fe9c3d44 80104722 80104722 ff8e6df4 ff8e6f60 ff8e6c58 - ntoskrnl.exe
fe9c3d4c 8012034c 8012034c #00000000 80088000 80106fc0 - ntoskrnl.exe

Restart and set the recovery options in the system control panel
or the /LDRASHDEBU0 system start option. If this message reappears,
contact your system administrator or technical support group.
    
```

BIOS

# System Management Mode

SMM Handler

HA application

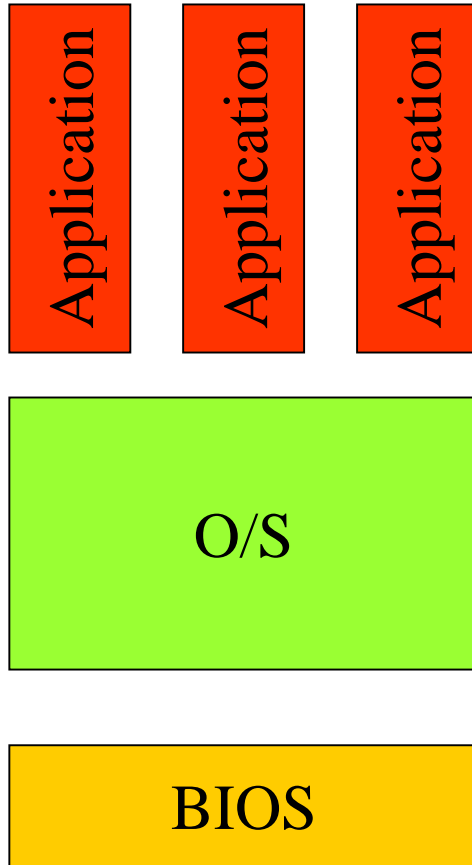
- email
- restart
- check for updates

SMM infrastructure including TCB

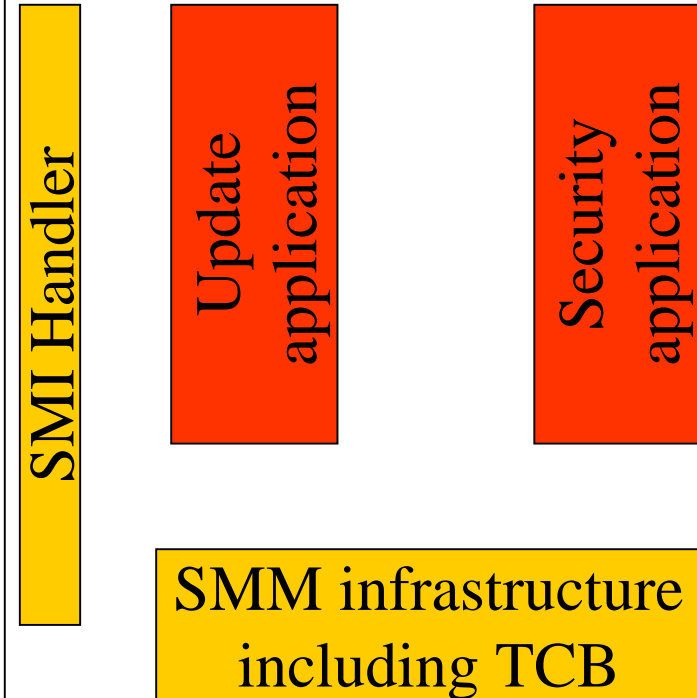
# Remote Management

- Perfect SMM application
- Update any upgradeable system component:
  - Disk partition
  - Files
  - CMOS contents
  - Flash memory
- Update authorization through security app

## Protected Mode



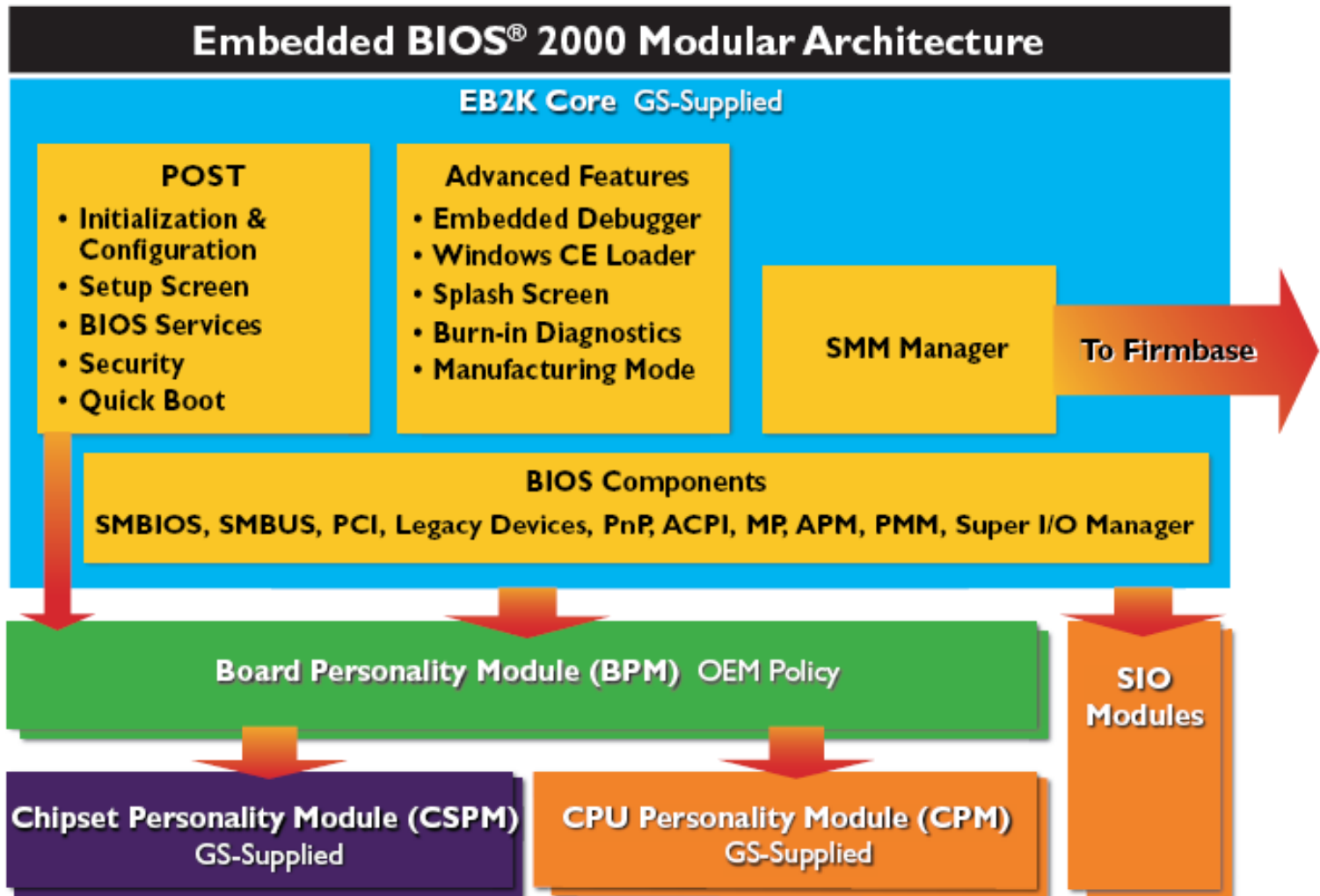
## System Management Mode



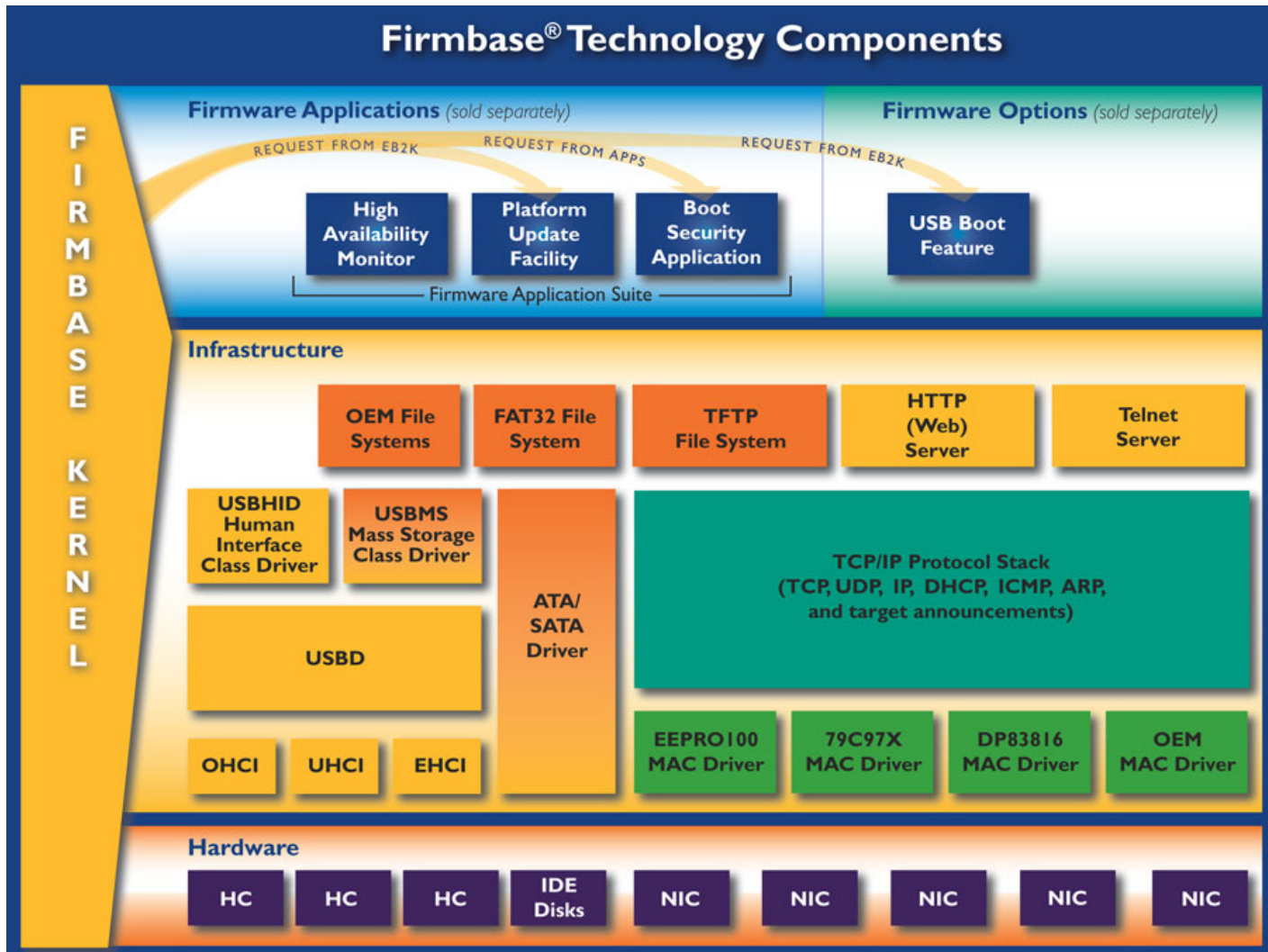
# Custom OEM Configurations

- Function of BIOS architecture
  - Modular architecture needed for ultimate configurability
- Need flexible way of adding value added firmware applications
- Need flexible way of adding custom initialization code

# Embedded BIOS<sup>®</sup> 2000



# Firmware® Technology



# Conclusion

- Digital Home devices
  - Full featured, yet affordable
  - Additional consumer requirements
  - Additional content/service provider requirements
- Understanding available technologies key to producing profitable solutions
- Reviewed some key market requirements
- Examined available solutions using Embedded BIOS<sup>®</sup> 2000 for VIA chipsets

[www.gensw.com](http://www.gensw.com)