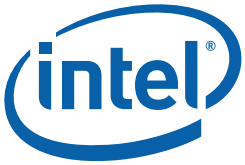


Firmware Hub to SPI Flash Conversion

Application Note

September 2008

Revision 001

Document Number: 320572-001US

‡ Intel® Active Management Technology (Intel® AMT) requires the platform to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see http://www.intel.com/technology/platform-technology/intel-amt/.

I2C* is a two-wire communications bus/protocol developed by Philips. SMBus is a subset of the I2C* bus/protocol and was developed by Intel. Implementations of the I2C* bus/protocol may require licenses from various entities, including Philips Electronics N.V. and North American Philips Corporation.

Contents

Figures

Tables

Revision History

Revision Number	Description	Revision Date
001	Initial release.	September 2008

§

1 Introduction

As new technology develops and the Industry drives the requirement to reduce board space and cost, companies are looking for improvements to effectively boot the system from the BIOS. Over the years the BIOS flash has migrated from the Industry Standard Architecture (ISA) bus to Low Pin Count (LPC) and now the industry is experiencing a move to Serial Peripheral Interface (SPI) flash. Beginning with the Intel® I/O Controller Hub 8 (ICH8) Family and the Intel® I/O Controller Hub 9 (ICH9) Family, platforms will start supporting both the LPC Firmware Hub (FWH) and firmware that is located in SPI flash. The movement of firmware from LPC to SPI may be driven by the lack of availability of the FWH devices.

SPI flash is becoming increasingly popular due to its low cost, small size, and fewer pins, allowing more devices to be placed on the mother board.

This intent of this paper is to help address some of the pitfalls when migrating from FWH boot Programmable Read Only Memory (PROM or EEPROM) to SPI Flash. The main focus will be on the system address decoding for memory-mapped flash accesses.

This paper will cover how the LPC maintains a path to the Super I/O and attachments for keyboard, mouse, floppy, non-volatile memory (NVM), and so forth, when considering booting from SPI flash.

Items not covered in this paper are design guidelines on the interface and device software programming. These are covered in the respective platform collateral.

Although examples illustrated in this paper focus on Intel® Xeon® Processor 5000 Sequence with Intel® 5100 Memory Controller Hub Chipset, the scope of material is applicable to all systems that use Intel ICH8/ICH9 and future Intel I/O controller hubs.

1.1 Terminology

Term	Description
GbE	Gigabit Ethernet
PROM	Programmable Read Only Memory
ISA	Industry Standard Architecture
FWH	Firmware Hub
LPC	Low Pin Count
SPI	Serial Peripheral Interface
ICH	I/O Controller Hub
TPM	Trusted Platform Module as defined by the Trusted Computing Group

1.2 Reference Documents

Document	Document No./Location
Intel® I/O Controller Hub 9 (ICH9) Family Datasheet	http://www.intel.com/Assets/PDF/datasheet/316972.pdf
Intel® 5100 Memory Controller Hub (MCH) Chipset Datasheet	http://www.intel.com/Assets/PDF/datasheet/318378.pdf
Intel® Xeon® Processor 5000 Sequence with Intel® 5100 Memory Controller Hub Chipset for Communications, Embedded, and Storage Applications Platform Design-In Presentation	CDI# 352119[1]
Intel® Xeon® Processor 5000 Sequence and Intel® 5100 Memory Controller Hub Chipset known as Tionesta Customer Reference Board (CRB) Schematics, Bill of Materials (BOM), and Layout Rev. 1.3	CDI# 350604[1]

[1] Please contact your Field Representatives to order this document

§

2 Typical System Topology

Figure 1. Development Kit for Intel® Xeon® Processor 5000 Sequence with Intel® 5100 Memory Controller Hub Chipset

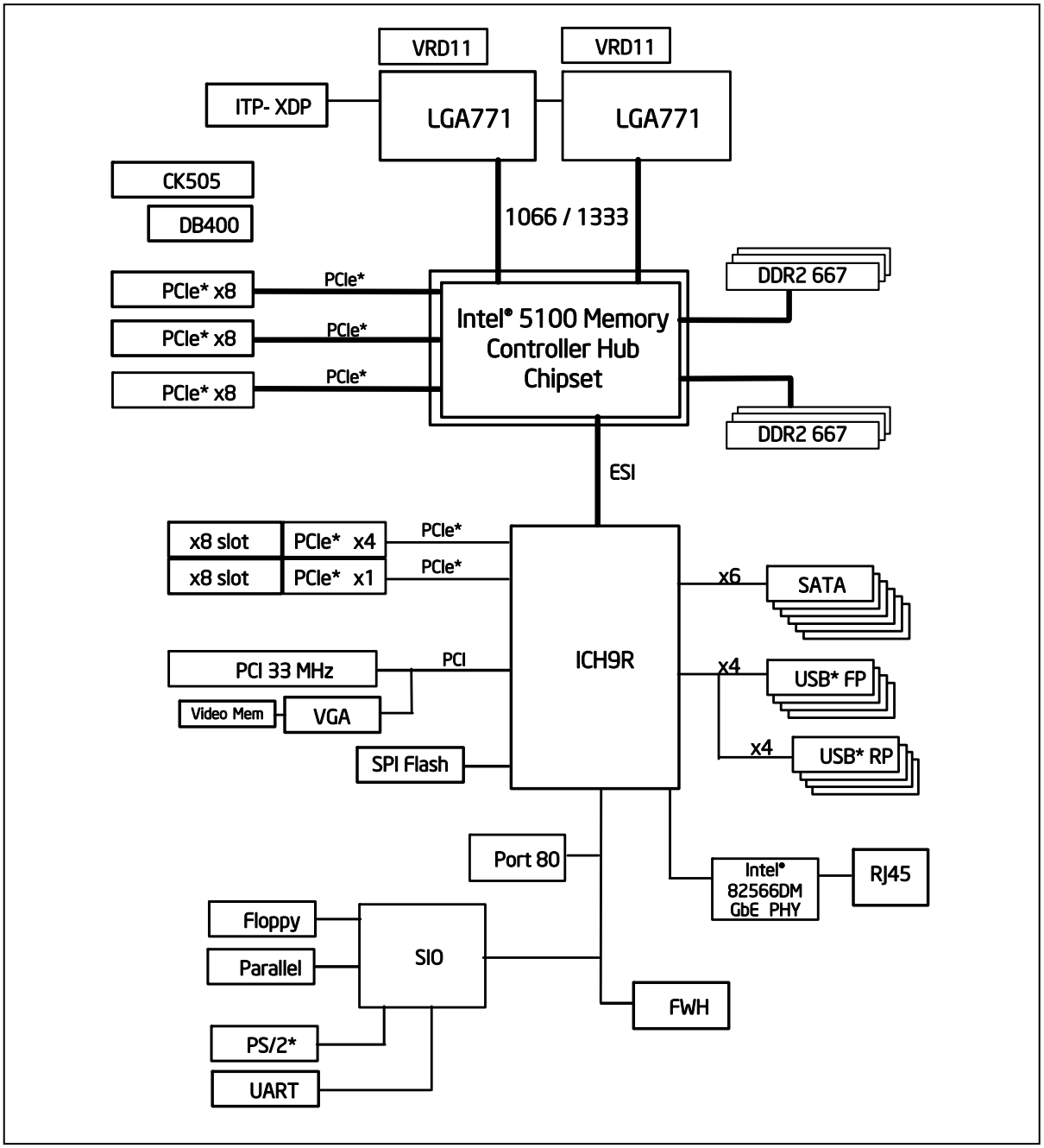


Figure 1 shows a typical board layout for Intel Architecture Systems. The Intel® MCH Chipset — sometimes referred to as the "northbridge" — handles high speed traffic between the processor and memory, processor and IO devices (PCI Express devices), and interacts with the Intel® ICH Chipset and its peripherals.

The Intel® ICH Chipset is sometimes referred to as the "southbridge". Its main purpose on the system board is to handle the slower devices and numerous IO peripherals support. The key bus interface of interest discussed in this paper is provided by Intel® ICH Chipset. Below is a snapshot of the SPI features that is supported by Intel® ICH9 Chipset specifically.

The SPI provides storage for the BIOS, the Intel® Management Engine (Intel® ME), and GbE. As the Intel Management Engine is not supported on this platform, it can be omitted from the SPI flash.

SPI Features

- 33 MHz clock support
    - Actual clock speeds are 17.86 and 31.25 MHz
- Fast read support
    - Devices with minimum of 33 MHz support
- Support for up to two SPI flash devices
    - Storage capacity may be different
    - Both devices must be from the same vendor and family
- Five configurable protection ranges
- Chipset soft straps supported only in SPI flash mode
- Max addressability is 16MB for each SPI device

§

3 System Address

3.1 Typical System Address

Figure 2. Intel® 5100 MCH Chipset System Address Map

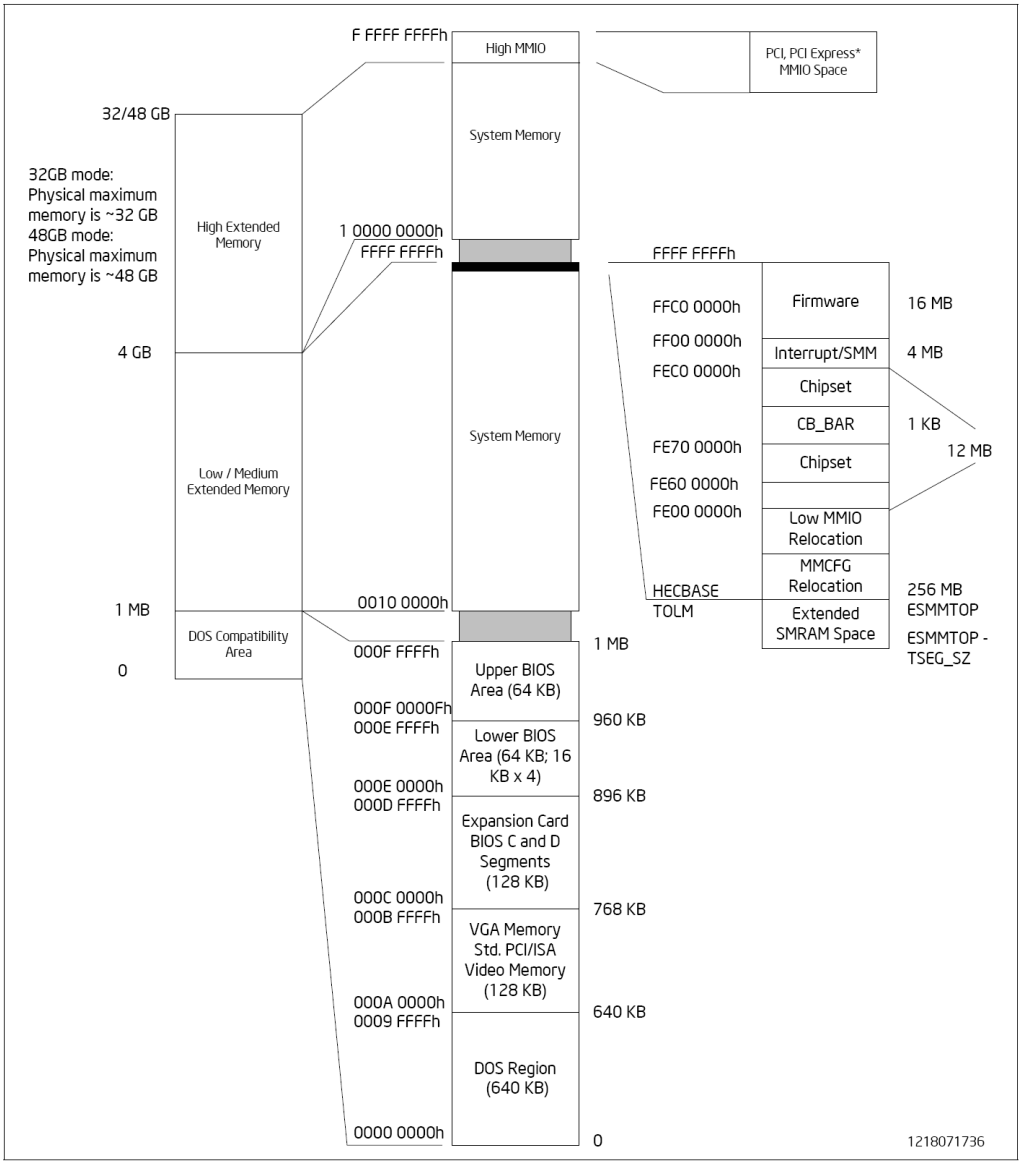
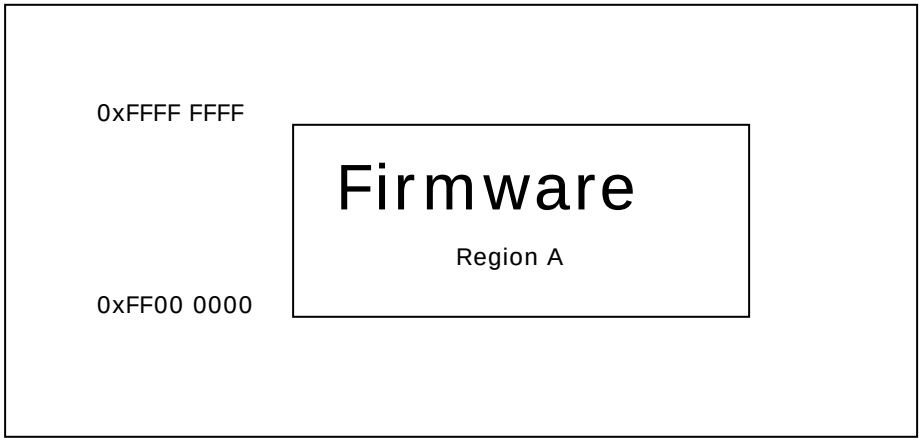


Figure 2 is taken from the Intel® 5100 MCH Chipset Datasheet. This figure serves as an example of a typical Intel Architecture System address mapping. A different chipset may provide some variation of this system address map. For details on each region, please refer to the Intel® 5100MCH Chipset Datasheet.

3.2 System Address Decoded to LPC

Figure 3. Address Map for Firmware



The above figure shows the system address range that will typically decode to system firmware. The firmware usually resides in the LPC bus inside the firmware hub component.

Let's label this system address range as Region A for discussion in this paper. In the next section, we will explore further the changes from the boot perspective that may affect system functionality with respect to the other components that need to be accessed through the memory map to Region A.

3.3 System Hardware Strap Functions

The system strap is typically sampled at boot time to allow for power on configuration of the system. In this section, we will discuss the relevant strap option available for select boot option on the system.

Since both the LPC bus and SPI are supported through the Intel® ICH Chipset, the ICH provides system address decoding of the firmware that is mapped to Region A. Thus, the ICH chipset will provide a mechanism to route access either to LPC or SPI after the system has booted.

There are two hardware pins (GNT0# and SPI_CS1#) on the ICH9 that will be sampled at the rising edge of PWROK signal to indicate to system whether to fetch the first instruction on the LPC or SPI or PCI. Once the system is strapped, all Region A access will go to LPC or SPI, or it will go to PCI only. For example if the system is booted with SPI strapped, memory access of Region A will never go to LPC or PCI.
The table below is taken from the From the Intel® I/O Controller Hub 9 (ICH9) Family Datasheet.

Table 1. Intel® ICH9 Boot Select Strap Option

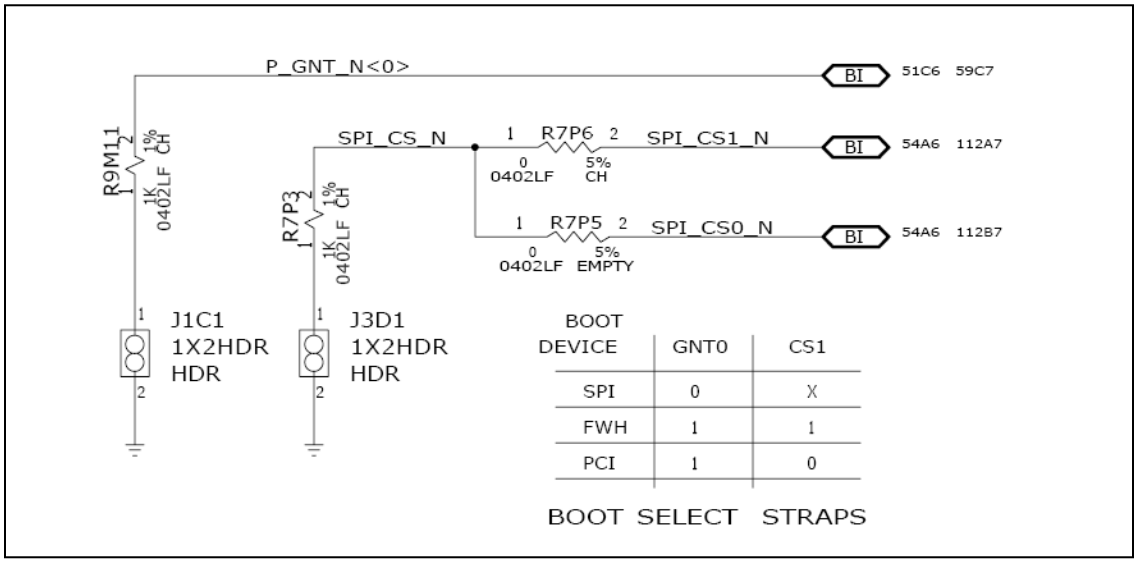
<table>
<tr><th>Signal</th><th>Usage</th><th>When Sampled</th><th>Comment</th></tr>
<tr><td>GNT0#</td><td>Boot BIOS Destination Selection 1</td><td>Rising Edge of PWROK</td><td>This field determines the destination of accesses to the BIOS memory range. Signals have weak internal pull-ups. Also controllable via Boot BIOS Destination bit (Chipset Config Registers:Offset 3410h:bit 11). This strap is used in conjunction with Boot BIOS Destination Selection 0 strap.
Bit11 (GNT0#) / Bit 10 (SPI_CS1#) / Boot BIOS Destination
0 / 1 / SPI
1 / 0 / PCI
1 / 1 / LPC
0 / 0 / Reserved

NOTE: Booting to PCI is intended for debug/testing only. Boot BIOS Destination Select to LPC/PCI by functional strap or via Boot BIOS Destination Bit will not affect SPI accesses initiated by Management Engine or Integrated GbE LAN.</td></tr>
<tr><td>SPI_CS1# / GPIO58 / CLGPIO6 (Digital Office Only)</td><td>Boot BIOS Destination Selection 0</td><td>Rising Edge of CLPWROK</td><td>This field determines the destination of accesses to the BIOS memory range. Signals have weak internal pull-ups. Also controllable via Boot BIOS Destination bit (Chipset Config Registers:Offset 3410h:bit 10). This strap is used in conjunction with Boot BIOS Destination Selection 1 strap.
Bit11 (GNT0#) / Bit 10 (SPI_CS1#) / Boot BIOS Destination
0 / 1 / SPI
1 / 0 / PCI
1 / 1 / LPC
0 / 0 / Reserved

NOTE: Booting to PCI is intended for debug/testing only. Boot BIOS Destination Select to LPC/PCI by functional strap or via Boot BIOS Destination Bit will not affect SPI accesses initiated by Management Engine or Integrated GbE LAN.</td></tr>
</table>

A sample implementation of strapped options for a Customer Reference Board known as a Development Kit for Intel® Xeon® Processor 5000 Sequence with Intel® 5100 Memory Controller Hub Chipset Platform Design Guidelines is shown below.

Figure 4. Strap Option for Tionesta Platform



As you can see from the implementation in this platform, the jumper settings will select the boot options, e.g., to boot from SPI or LPC or PCI. The user can change the boot option before powering up the system. If the user wants to boot with SPI flash, the J1C1 will need to be connected to pull the GNT0 low. Otherwise, keep the J1C1 open will boot up with LPC FWH option. For your information, these GNT0# and SPI_CS1# signals as noted in Table 1 have weak internal pull up. Thus the SPI_CSI_N signal is not pulled up physically on the platform board schematics.

§

4 Things to Consider

As mentioned in the earlier sections, we need to be aware that when the system is strapped to boot from SPI flash, the Region A will no longer be decoded to the LPC interface. The strap is sampled at boot time and cannot be changed dynamically when the system is operational.

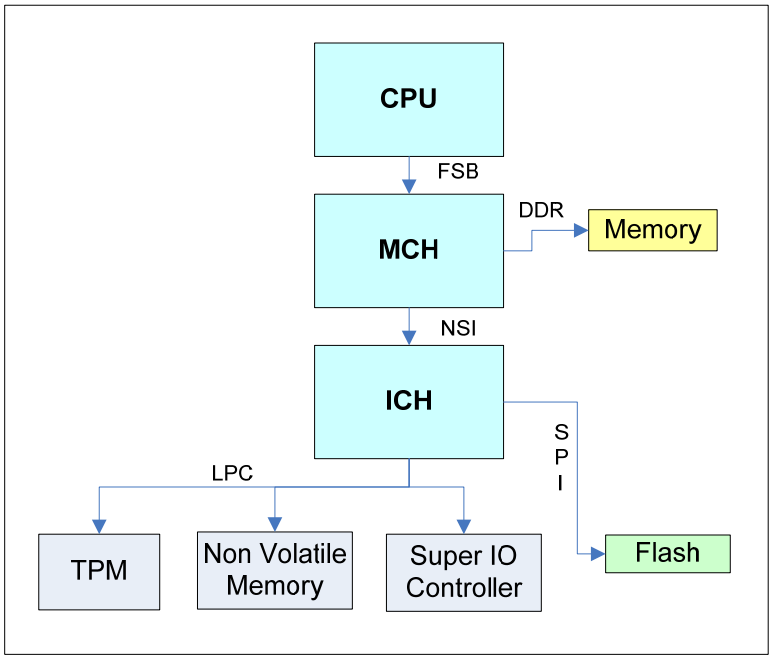
Some systems are designed to support both SPI flash and LPC FWH. These systems provide jumpers on board to configure the system to select the boot device. If the system is strapped to boot from LPC FWH, then all of the system addresses in Region A will be decoded and send to the LPC devices. Alternatively, if it is strapped to boot from the SPI flash, the SPI flash component will have to hold the system firmware to boot the system. In this case, none of the system addresses in Region A will be decoded to the LPC interface.

During system migration, it is easy enough to have the entire system firmware migrate to a SPI device. Unfortunately there are other software considerations for devices that are located on the LPC interface within the system besides the boot flash. For example the super I/O component, the non-volatile memory, and the TPM component can still function off the LPC bus.

In this section, let's consider the following two system topologies with respect to non-volatile memory. In both topologies the systems are strapped to boot with SPI flash. The main focus is how accesses will affect other components on the LPC bus such as the super I/O and TPM components on the LPC bus.

4.1 System Topology 1

Figure 5. T-Topology on LPC Bus

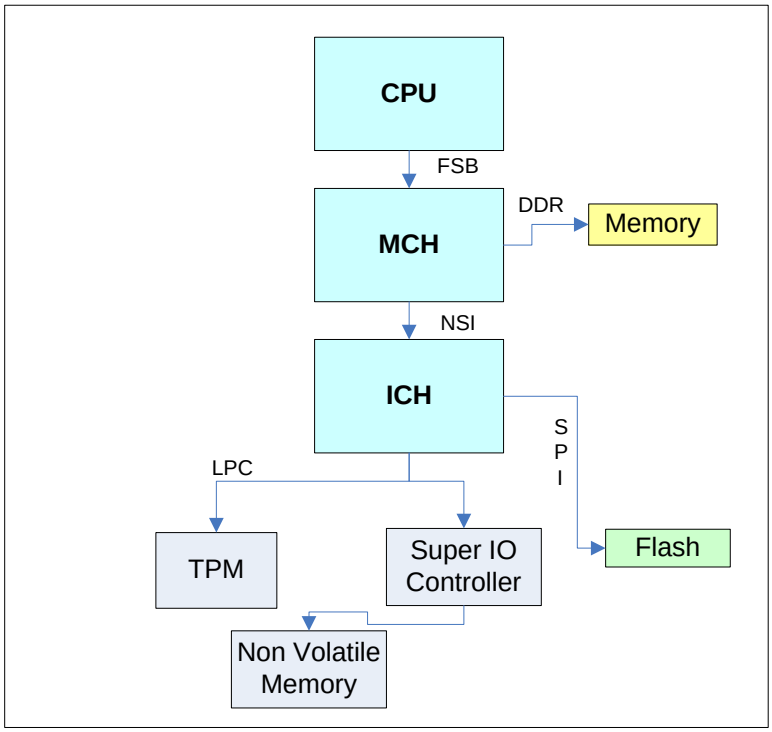


With the above system topology, all of the I/O accesses on the LPC bus will continue to function. I/O access and I/O DMA to LPC components that support such operations will still function normally. Regular memory reads and writes on the LPC bus to Region A will not be broadcast on the LPC bus.

With this system topology, any software that performs memory map I/O read and write accesses (Region A) will be affected. To overcome this issue, system software that access these NVM device will have to be rewritten to perform I/O reads or writes, I/O DMA, and so forth. With this methodology change, the system may experience performance implications for such an access and system software developers will have to include bake in time and validation effort for this implementation.

4.2 System Topology 2

Figure 6. Daisy Chain Topology on LPC Bus



With the above system topology shown in Figure 6, all of the I/O accesses on the LPC bus will continue to function. I/O accesses and I/O DMA to the LPC components that support such operations will also continue to function normally. Regular memory reads and writes on LPC bus to Region A will not be broadcast on the LPC bus.

The only difference on this system topology versus the T-Topology discussed earlier is that the super I/O controller may provide support of extended memory map access to the non-volatile memory component. Even so, the extended memory map region is a subset of system memory in Region A. Since Region A access does not broadcast on the LPC bus, the memory-mapped I/O read and write accesses to non-volatile memory are affected.

To overcome this issue, system software that accesses these NVM devices will have to be rewritten to perform I/O reads or writes, I/O DMA, and so forth. With this methodology, the system may experience performance implications for such an access and system software developers will need to consider the validation effort for this implementation.

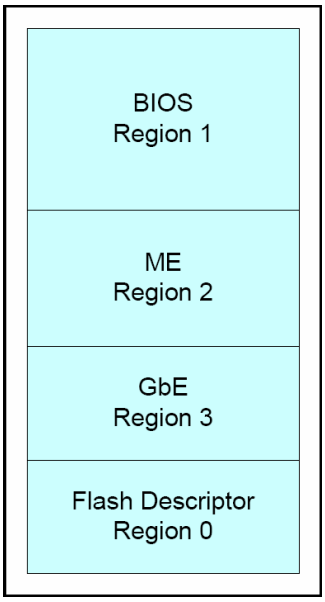
4.3 Other Options

In an earlier section, this paper has emphasized that the memory mapped I/O read and I/O write to Region A for LPC components may be affected when the system boot of SPI flash is selected. Additionally the firmware that uses these accesses will need modification either by performing I/O reads and writes or I/O DMA. In the following section, other alternatives that may be considered for system implementation will be discussed.

4.3.1 SPI Flash Memory as Storage

SPI flash is partitioned into a few regions: the BIOS region, the Intel ME region, the GbE region, and the Flash Descriptor region.

Figure 7. SPI Flash Partitions



For a system that does not utilize or support the integrated Intel Management Engine (Intel ME), the Intel ME region 2 above in SPI flash can be disabled or used for platform storage. This method would serves as another option to overcome the memory mapped I/O read and write access to Region A.

4.3.2 Memory Access to TPM Open Region

There is a subset of memory mapped I/O access that will still be broadcast on the LPC bus. This memory region is meant for access to a discrete TPM component typically located on the LPC bus. Memory addresses 0xFED4 0000h – 0xFED4 BFFFh are still enabled when booting from SPI flash.

Table 2. Intel® ICH9 Memory Decode Range from Host Perspective

Memory Range	Target
0xFED4 0000h – 0xFED4 BFFFh	TPM on LPC

Even through this memory range decodes to TPM on LPC, there is only a small window of 4KB from 0xFED4 0000h to 0xFED4 0FFCh that can be read and written. This is due to the Locality Level as defined by Trusted Computing Group (TCG) for Trusted Platform Module version 1.2.

To utilize this option, the LPC component will need to support the LT_READ and LT_WRITE functionality on the LPC bus.

§

5 Summary

As the industry drives towards LPC FWH to SPI flash conversion, this paper identifies some of the things to consider during this activity. This paper is not intended to provide a complete list of issues that you may encounter during this transition, so for specific design guidelines for a platform, please refer to its respective platform collateral for details.

In conclusion, the information provided here may be something that is not being considered during the design conversion process. Thus this information may be useful if you have designs similar to those outlined in the two design topologies on the LPC bus. This paper is intended to raise SPI flash conversion awareness for readers early in the design process to avoid any unnecessary delay in bringing products to end users.

§