

IP Independent Generic Firmware to accelerate Development Process Iteration

Submitted by

Gahan Saraiya

18MCEC10



Department of Computer Science & Engineering,
Institute of Technology,
Nirma University, Ahmedabad,
Gujarat - 382481, India.

May, 2020

IP Independent Generic Firmware to accelerate Development Process Iteration

Major Project

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Computer Science & Engineering
with specialization in Computer Science & Engineering

Submitted by

Gahan Saraiya

18MCEC10



Department of Computer Science & Engineering,
Institute of Technology,
Nirma University, Ahmedabad,
Gujarat - 382481, India.



Declaration

I hereby declare that the dissertation ***IP Independent Generic Firmware to accelerate Development Process Iteration*** submitted by me to the Institute of Technology, Nirma University, Ahmedabad, 382481 in partial fulfillment of the requirements for the award of **Master of Technology in Computer Science & Engineering with specialization in Computer Science & Engineering** is a bona-fide record of the work carried out by me under the supervision of **Prof. Dvijesh Bhatt**.

I further declare that the work reported in this dissertation, has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma of this institute or of any other institute or University.

Sign:

Name & Roll. No.:

Date:



Computer Science & Engineering

Certificate

This is to certify that the dissertation entitled ***IP Independent Generic Firmware to accelerate Development Process Iteration*** submitted by ***Gahan Saraiya*** (Roll No. 18MCEC10) to Nirma University Ahmedabad, in partial fulfillment of the requirement for the award of the degree of **Master of Technology** in **Computer Science & Engineering with specialization in Computer Science & Engineering** is a bona-fide work carried out under my supervision. The dissertation fulfills the requirements as per the regulations of this University and in my opinion meets the necessary standards for submission. The contents of this dissertation have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma and the same is certified.

Prof. Dvijesh Bhatt
Guide & Assistant Professor,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Priyanka Sharma
Professor,
Coordinator M.Tech - CSE (CSE)
Institute of Technology,
Nirma University, Ahmedabad

Dr. Madhuri Bhavsar
Professor and Head,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. R. N. Patel
I/C Director,
Institute of Technology,
Nirma University, Ahmedabad

Abstract

Intel System on a Chip (SoC) features a new set of Intel Intellectual Property (IP) for every generation. BIOS involves development of major individual components such as Processor, Graphics/Memory Controller, Input/Output Controller hub, System Monitor/Management Bus, Direct Media Interface, SATA/IDE/USB, Peripheral Component Interconnect (PCI), Voltage Regulator and Advanced Configuration and Power Interface (ACPI) for every Intel System on a Chip (SoC). Section 1. describes all the basic information required on the Intel SoC.

Section 2. involves the design of the Basic Boot Flow of the BIOS followed by Section 3. and Section 4. explains the architecture and protocols which are the concept used to build the proposed framework which is described under Section 5. to aid the development and debugging iteration for various stakeholders including but not limited to BIOS Developers, Validation Engineers, Automation team.

The framework is designed and implemented to aid the development process by eliminating longer duration of common debugging steps and providing a sophisticated way to build and test the various scenarios includes but not limited to Setup Options, Firmware Flashing, UEFI Variable Creation.

Acknowledgements

It gives me immense pleasure in expressing thanks and profound gratitude to Prof. Dvijesh Bhatt, Assistant Professor, Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his valuable guidance and continual encouragement throughout this work. The appreciation and continual support he has imparted has been a great motivation to me in reaching a higher goal. His guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

It gives me an immense pleasure to thank Dr. Madhuri Bhavsar, Honorable Head of Computer Science And Engineering Department, Institute of Technology, Nirma University, Ahmedabad for her kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed whole heartedly to Dr. Alka Mahajan, Honorable Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation she has extended throughout course of this work. I would also thank the Institution, all faculty members of Computer Engineering Department, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

Gahan Saraiya

18MCEC10

Contents

Declaration	ii
Certificate	iii
Abstract	iv
Acknowledgements	v
List of Figures	ix
1. Introduction	1
1.1 Uncore IP	1
1.2 Legacy BIOS and UEFI	1
BIOS	1
1.2.1 Background of Legacy BIOS	2
1.2.2 Limitations of legacy BIOS	2
1.3 Unified Extensible Firmware Interface (UEFI)	2
1.3.1 UEFI Driver Model Extension	3
1.3.2 UEFI's Role in boot process	4
1.4 Comparing of Legacy BIOS and UEFI	4
1.5 Advanced Configuration and Power Interface (ACPI)	4
1.5.1 Overview of ACPI Subsystem	5
1.5.2 OS-independent ACPI Subsystem	7
1.5.3 Operating System Services Layer	7
1.5.4 ACPI Subsystem Interaction	8
1.6 Peripheral Component Interconnect Express (PCIe)	8
1.6.1 Functional Description	10
1.6.2 UEFI PCI Services	10
1.6.3 UEFI Driver Model	10
1.6.4 Graphics Output Protocol (GOP)	11
1.6.5 BUS Performances and Number of Slots Compared .	11
1.7 Graphics Controller	12
1.7.1 Graphics Output Protocol	13

1.7.2	GOP Overview	13
1.7.3	GOP DRIVER	14
1.7.4	GOP Integration	14
2.	Design	16
2.1	UEFI Design Overview	16
2.1.1	UEFI Driver Goals	17
2.2	UEFI/PI Firmware Images	18
2.3	Platform Initialization PI Boot Sequence	20
2.4	Security (SEC)	21
2.5	Pre-EFI Initialization (PEI)	22
2.5.1	PEI Services	23
2.5.2	PEI Foundation	23
2.6	PEI Dispatcher	25
2.7	Drive Execution Environment (DXE)	25
2.8	Boot Device Selection (BDS)	25
2.9	Transient System Load (TSL) and Runtime (RT)	26
2.10	After Life (AL)	26
2.11	Generic Build Process	26
2.11.1	EFI Section Files	27
2.12	Cross Compatibility of CPUs	27
3.	Architecture of BIOS Firmware	30
3.1	Overview	30
3.2	Design of Firmware Storage	30
Firmware Device	30	
Flash	30	
3.3	Firmware Volume (FV)	31
3.4	Firmware File System (FFS)	31
3.4.1	Firmware File Types	33
3.5	Firmware File Section	33
3.6	Firmware File Section Types	35
3.7	PI Architecture Firmware File System Format	35
3.7.1	Firmware Volume Format	38
3.7.2	Firmware File System Format	38
Firmware File System GUID	38	
Volume Top File	39	
3.8	Firmware File Format (FFS)	39
3.9	Firmware File Section Format	39
3.10	File System Initialization	40
3.11	Traversal and Access to Files	41
Note	42	
3.12	File Integrity and State	42
4.	System Management Mode (SMM)	44
4.1	Overview	44

4.2	System Management System Table (SMST)	44
4.3	SMM and Available Services	45
4.3.1	SMM Services	45
4.3.2	SMM Library	45
4.4	SMM Drivers	46
4.4.1	Process to Load Drivers in SMM	46
4.4.2	SMM Drivers for IA-32	46
4.4.3	"Itanium® Processor Family" SMM Drivers	47
4.5	SMM Protocols	47
4.5.1	SMM Protocols for IA-32	47
4.5.2	SMM Protocols for "Itanium®-Based Systems"	48
4.6	SMM Dispatcher and infrastructure	48
4.7	Initializing SMM Phase	48
4.8	Relation of "System Management RAM (SMRAM)" to conventional memory	49
4.9	Execution Mode of SMM on Processor	49
4.10	Accessing Platform Resources	50
5.	Proposed Work	51
5.1	Stake holders	51
5.2	Issues	51
5.3	Requirements	52
5.3.1	Software Requirements	52
5.4	Development Process of Modules	52
5.5	Module: Setup Knob modification	52
5.5.1	Processing Unsigned debug BIOS	52
5.5.2	Additional Tech Stack Used	53
5.5.3	Flow of the module	53
5.5.4	Screenshots of Module	53
5.5.5	Outcome of Module	55
5.6	Module: Parsing	56
5.6.1	Additional Tech Stack Used	56
5.6.2	Flow of the module	58
5.6.3	Outcome of Module	58
5.7	Module: Runtime UEFI variable Creation	59
5.7.1	Additional Tech Stack Used	59
5.7.2	Flow of the module	59
5.7.3	Screenshots of Module	60
5.7.4	Outcome of the module	64
6.	Future Scope of Work	67

List of Figures

1	Board of Directors of UEFI Forum	3
2	The ACPI Component Architecture	6
3	ACPICA Subsystem Architecture	8
4	Interaction between the Architectural Components	9
5	UEFI Conceptual Overview	16
6	UEFI/PI Firmware Image Creation	19
7	UEFI/PI Firmware Image Creation	20
8	PI Boot Phases	21
9	Diagram of PI Operations	23
10	General EFI Section Format for large size Sections(greater then 16 MB)	27
11	General EFI Section Format (less then 16 MB)	27
12	Cross Compatibility Design	28
13	BIOS Support for Cross Compatibility	28
14	Integrated Firmware Image	29
15	Firmware File Type	34
16	Example File System Image	37
17	The Firmware Volume Format	38
18	Layout representation of FFS File Header ($\leq 16Mb$)	40
19	Layout representation of FFS File Header 2 layout for files ($> 16Mb$)	40
20	Section Header Format when $size < 16Mb$	41
21	Section Header Format of when $size \geq 16Mb$ using Extended Length field	41
22	SMM Framework Architecture	44
23	Protocols Published for IA-32 Systems	47
24	Protocols Published for "Itanium®-Based Systems"	48
25	SMRAM kinship with conventional memory	49
26	Flow of Setup Knobs Modification	54
27	Menu to Select initial configuration for work	55
28	Available work mode for the system: Online and Offline	55
29	Overview of BIOS image as a File System	57
30	Flow of Parser	58
31	Flow of Nvar Web GUI	60
32	Home Page to Create UEFI Variable	61
33	Variables created or exists on SUT	62

34	Create new UEFI Variable on SUT	62
35	Options listed under Variable	63
36	Edit the Existing Option Created under Variable SUT	63
37	Create New Option(s) under Variable - Oneof Type	64
38	Create New Option(s) under Variable - String Type	64
39	Create New Option(s) under Variable - Numeric Type	65
40	Create Reserved Space for future use under Variable	65
41	Generate XML SUT	66
42	Generate XML SUT	66

1. Introduction

Intel System on a Chip (SoC) features a new set of Intel Uncore Intellectual Property (IP) for every generation. Section 1. covers the introduction and overview of BIOS, UEFI and it's role and major components - Advanced Configuration and Power Interface (ACPI), Peripheral Component Interconnect Express (PCIe) and Graphics Controller. Section 2. describes the design of UEFI and the boot phases in detail. The study of the BIOS binary structure and mapping of each components byte and alignment is described in Section 3.. Proposed work to reducing the process of build iteration described in Section 5..

1.1 Uncore IP

The Uncore encompasses system agent (SA), memory and Uncore agents such as graphics controller, display controller, memory controller and Input Output (IO). The Uncore IPs are Peripheral Component Interface Express (PCIe), Graphics Processing Engine (GPE), Thunderbolt, Imaging Processing Agent (IPU), North Peak (NPK), Virtualization Technology for directed-IO (Vt-d), Volume Management Device (VMD).

PCI Express abbreviated as PCI or PCIe, is designed to replace the older PCI standards. A data communicating system is highly-developed via PCIe for use the transfer data between the host and the peripheral devices. Intel developed the hardware interface which allows the connection of external peripherals to a computer called Thunderbolt. This interface not only has PCI Express (PCIe) and DisplayPort (DP) combined into two serial signals but additionally provides DC power also, bundled in just one cable. "Graphics Processing Engine (GPE)", "Integrated graphics", "shared graphics solutions", "integrated graphics processors (IGP)" or "unified memory architecture(UMA)" utilize a portion of a memory of computer system instead of having dedicated graphics memory. GPEs can be integrated onto the motherboard as part of the chipset. Guest virtual machines use Virtual Technology for Directed-IO (Vt-d), an input/output memory management unit(IOMMU), to directly use peripheral devices, such as hard-drive controllers, accelerated graphics cards and Ethernet, through interrupt remapping.

1.2 Legacy BIOS and UEFI

BIOS is the governing reference which specifies a firmware interface.

"Legacy" (as in Legacy BIOS) - in terms of firmware specifications it refers to an older, broadly used specification. Major responsibility of BIOS is to initialize the hardware devices, loading and commencing an OS. When the system boots, the BIOS initializes and identifies every connected system devices including keyboard, mouse, hard disk drive, solid state drive, video display card and other hardware followed by locating software stored on a boot device i.e. a hard disk or removable

storage such as USB or CD/DVD and loads and executes that software, transferring control of the system to it. This flow of actions is also known as "booting" or "boot strapping".

1.2.1 Background of Legacy BIOS

In 1980s, IBM developed the personal computer with a 16-bit BIOS with the aim of ending the BIOS after the first 250,000 products. Legacy BIOS is based upon Intel's original 16-bit architecture, ordinarily referred to as "8086" architecture. And as technology advanced, Intel extended that 8086 architecture from 16 to 32-bit. Legacy BIOS is able to run different OS very well irrespective if the system is IBM or not. Additionally, Legacy BIOS also has a defined OS-independent interface for hardware that enables interrupts to communicate with keyboard, disk and video services along with the BIOS ROM loader and bootstrap loader, to name a few.

Use of legacy BIOS is diminishing and is expected to be phased out in new systems by the year 2020.

1.2.2 Limitations of legacy BIOS

With progress in technologies, the BIOS implementations were also updated with many new configuration and power management technologies and added support for many generations of Intel® architecture hardware. Although a few of limitations namely, upper memory block (UMB) dependencies, PC AT hardware dependencies, 1 MB addressable space and 16-bit addressing mode persisted throughout the years. The need to integrate libraries of third-party firmware modules into a single platform solution across multiple product lines and ensuring quality of individual firmware modules arises in the industries. The existing market demands to overcome inherent limitations lead towards development of a fresh BIOS architecture which is introduced in market as The UEFI specifications.

One major problem with existing BIOS implementations is that since they are highly customized for a specific motherboard, there maintenance is difficult. A lot of effort is required in significant porting, integration, testing and debug work of changes in component modules. The UEFI architecture is designed to considering these limitations and to resolve them.

1.3 Unified Extensible Firmware Interface (UEFI)

UEFI is a replacement for legacy BIOS to act as the interface between a operating system and its platform firmware streamlining the booting process. It offers a rich extensible pre-OS environment with advanced boot and runtime services, replacing most BIOS functions. Unified Extensible Firmware Interface (UEFI) is grounded in

Intel's initial Extensible Firmware Interface (EFI) specification 1.10, which defines a software interface between an operating system and platform firmware. It has intrinsic networking capabilities, is designed to work with multi-processors (MP) system and also allows users to execute applications on a command line interface.

MARK DORAN President Intel	DONG WEI Vice President ARM	JEFF BOBZIN Secretary Insyde Software	BILL KEOWN Treasurer Lenovo
			
WILLIAM MOYES Advanced Micro Devices, Inc.	STEFANO RIGHI American Megatrends, Inc.	ANDREW FISH Apple	ANAND JOSHI Dell
			
KEVIN DEPEW Hewlett Packard Enterprise	RICK BRAMLEY HP, Inc.	JEREMY KERR IBM	TOBY NIXON Microsoft
			
DICK WILKINS Phoenix Technologies			

FIGURE 1: Board of Directors of UEFI Forum

The UEFI Forum board of directors consists of representatives from 11 industry leaders as described in Figure 1. These organizations work to ensure that the UEFI specifications meet industry needs.

UEFI uses a different interface for runtime services and boot services but UEFI does not specify how "Power On Self Test" (POST) and Setup are implemented those are BIOS' primary functions.

1.3.1 UEFI Driver Model Extension

Boot devices are accessible via a set of protocol interfaces. The UEFI Driver Model provides a replacement for PC-AT-style option ROMs.

The UEFI Driver Model was not designed to replace the high-performance OS specific drivers but to access boot devices in the pre-boot environment, to support the execution of modular pieces of code, also known as drivers. These drivers control hardware buses and devices on the platform, and also they may provide some software-derived, platform specific service. The information required by the driver

developers for implementing combination of bus drivers which boot an UEFI-compliant OS are included in the UEFI Driver Model.

Thus the UEFI Driver Model is designed to be generic. The UEFI Specification describes how to write USB bus drivers, USB device drivers, PCI device drivers, PCI bus drivers and SCSI drivers. Additional details are provided that allow UEFI drivers to be stored in PCI option ROMs, while maintaining compatibility with legacy option ROM images.

The UEFI Specification is designed keeping in mind the goal of having compact driver images. However to facilitate support for multiple processor architectures, a driver object file for each architecture is required to be included leading to a space issue. To resolve this issue, UEFI defines EFI Byte Code Virtual Machine. Every driver file is compiled into just a single EFI Byte Code object which is run by an UEFI Byte Code Interpreter included in the UEFI Specification compliant firmware. Another very common method to resolve this issue is compression. The UEFI specification defined compression and decompression algorithms which may be used to reduce the size of UEFI Drivers.

This information can be used by OEMs, IHBs, OSVs, and firmware vendors for developing drivers that produce standard protocol interfaces, and operating system loaders that can be used to boot UEFI compliant operating systems.

1.3.2 UEFI's Role in boot process

During the boot process, UEFI speaks to the operating system loader and acts as the interface between the operating system and the BIOS.

The PC-AT boot environment is challenging to innovate as each new firmware capability requires firmware developers to craft more complex solutions, often requiring OS developers to make changes to their boot code. Since this is a time-consuming process and also required investment of resources, the UEFI specification undertakes it as a primary goal to overcome this issue.

1.4 Comparing of Legacy BIOS and UEFI

1.5 Advanced Configuration and Power Interface (ACPI)

The ACPI Component Architecture (ACPI) defines and implements a group of software components that together create an implementation of the ACPI specification. A major goal of the architecture is to isolate all operating system dependencies to a relatively small translation or conversion layer (the OS Services Layer) so that the bulk of the ACPI code is independent of any individual operating system. Therefore, hosting the ACPI code on new operating systems requires no source changes within the ACPI code itself.

TABLE 1: Comparison of Legacy BIOS and UEFI

	Legacy BIOS	EFI
Programming Language used	Assembly Language	C Language (99%)
Resources	Interrupt Hardcode Memory Access hardcore Input/Output Access	Divers, Handlers and Protocols
Processor Type	$x86\ 16-bit$	CPU Protects Mode
Expand	Interrupt through hook	Driver to be loaded
OS Communication Bridge	via ACPI	through runtime driver
3 rd Party ISV & IHV	Support Bas	Ease of Support and for Cross-Platforms

The components of the architecture include:

- An OS-independent, kernel-resident ACPICA Subsystem component that provides the fundamental ACPI services such as the AML interpreter and namespace management.
- An OS-dependent OS Services Layer for each host operating system to provide OS support for the OS-independent ACPICA Subsystem.
- An ASL compiler-disassembler for translating ASL code to AML byte code and for disassembling existing binary ACPI tables back to ASL source code.
- Several ACPI utilities for executing the interpreter in ring 3 user space, extracting binary ACPI tables from the output of the ACPI Dump utility, and translating the ACPICA source code to Linux/Unix format.

In Figure 2, the ACPICA subsystem is shown in relation to the host operating system, device driver, OSPM software, and the ACPI hardware

1.5.1 Overview of ACPICA Subsystem

The ACPICA Subsystem implements the low level or fundamental aspects of the ACPI specification. Included are an AML parser/interpreter, ACPI namespace management, ACPI table and device support, and event handling. Since the ACPICA subsystem provides low-level system services, it also requires low-level operating

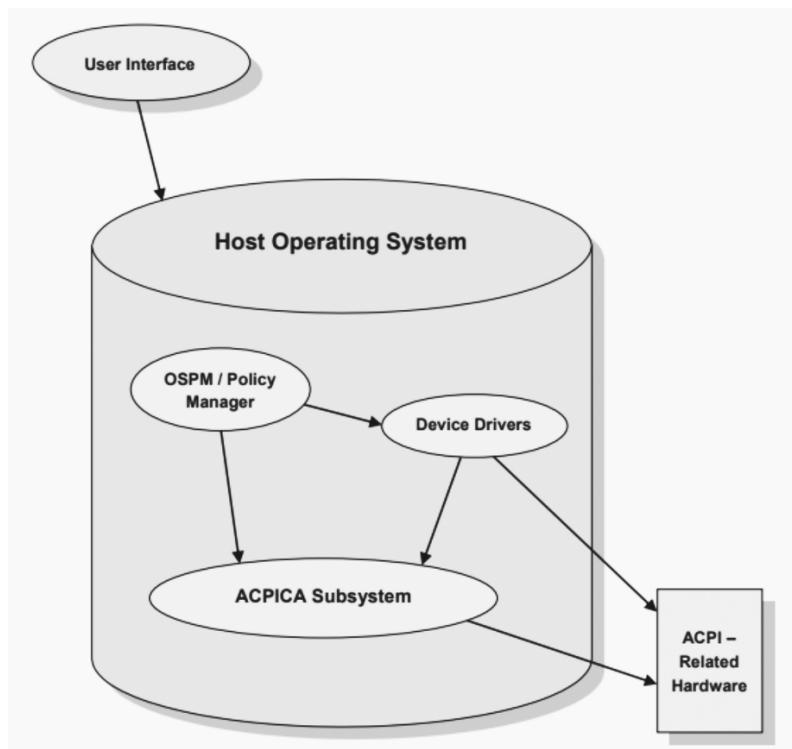


FIGURE 2: The ACPI Component Architecture

system services such as memory management, synchronization, scheduling, and I/O.

To allow the ACPI Subsystem to easily interface to any operating system that provides such services, an Operating System Services Layer translates ACPI-to-OS requests into the system calls provided by the host operating system. The OS Services Layer is the only component of the ACPI that contains code that is specific to a host operating system.

Thus, the ACPI Subsystem consists of two major software components:

- The basic kernel-resident ACPI Subsystem provides the fundamental ACPI services that are independent of any particular operating system.
- The OS Services Layer (OSL) provides the conversion layer that interfaces the OS independent ACPI Subsystem to a host operating system.

When combined into a single static or loadable software module such as a device driver or kernel subsystem, these two major components form the ACPI Subsystem. Throughout this document, the term "ACPI Subsystem" refers to the combination of the OS-independent ACPI Subsystem with an OS Services Layer components combined into a single module, driver, or load unit.

1.5.2 OS-independent ACPI Subsystem

The OS-independent ACPI Subsystem supplies the major building blocks or sub-components that are required for all ACPI implementations — including an AML interpreter, a namespace manager, ACPI event and resource management, and ACPI hardware support.

One of the goals of the ACPI Subsystem is to provide an abstraction level high enough such that the host operating system does not need to understand or know about the very low-level ACPI details. For example, all AML code is hidden from the host. Also, the details of the ACPI hardware are abstracted to higher-level software interfaces.

The ACPI Subsystem implementation makes no assumptions about the host operating system or environment. The only way it can request operating system services is via interfaces provided by the OS Services Layer.

The primary user of the services provided by the ACPI Subsystem are the host OS device drivers and power/thermal management software.

1.5.3 Operating System Services Layer

The OS Services Layer (or OSL) operates as a translation service for requests from the OS independent ACPI subsystem back to the host OS. The OSL implements a generic set of OS service interfaces by using the primitives available from the host OS. Because of its nature.

The OS Services Layer must be implemented anew for each supported host operating system. There is a single OS-independent ACPI Subsystem, but there must be an OS Services Layer for each operating system supported by the ACPI component architecture.

The primary function of the OSL in the ACPI Component Architecture is to be the small glue layer that binds the much larger ACPI Subsystem to the host operating system. Because of the nature of ACPI itself — such as the requirement for an AML interpreter and management of a large namespace data structure — most of the implementation of the ACPI specification is independent of any operating system services. Therefore, the OS-independent ACPI Subsystem is the larger of the two components.

The overall ACPI Component Architecture in relation to the host operating system is Figure

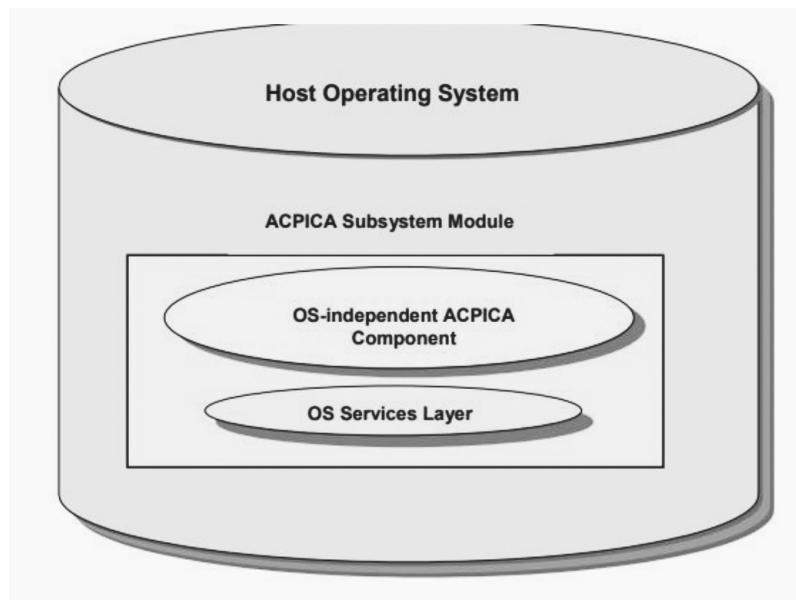


FIGURE 3: ACPICA Subsystem Architecture

1.5.4 ACPICA Subsystem Interaction

The ACPICA Subsystem implements a set of external interfaces that can be directly called from the host OS. These Acpi* interfaces provide the actual ACPI services for the host. When operating system services are required during the servicing of an ACPI request, the Subsystem makes requests to the host OS indirectly via the fixed AcpiOs* interfaces. The diagram below illustrates the relationships and interaction between the various architectural elements by showing the flow of control between them. Note that the OS-independent ACPICA Subsystem never calls the host directly instead it makes calls to the AcpiOs * interfaces in the OSL. This provides the ACPICA code with OS-independence.

The Interaction between the Architectural Components is shown in Figure 4

1.6 Peripheral Component Interconnect Express (PCIe)

The PCI architecture has proven to be successful beyond even the most optimistic expectations. Today nearly every new computer platform comes outfitted with multiple PCI slots. In addition to the unprecedented number of PCI slots being shipped, there are also hundreds of PCI adapter cards that are available to satisfy virtually every conceivable application. This enormous momentum is difficult to ignore.

Today there is also a need for a new, higher-performance I/O interface to support emerging, ultrahigh-bandwidth technologies such as 10 Gigabit Ethernet, 10 Gigabit FibreChannel, 4X and 12X InfiniBand, and others. A standard that can meet these performance objectives, while maintaining backward compatibility to previous generations of PCI would undoubtedly provide the ideal solution.

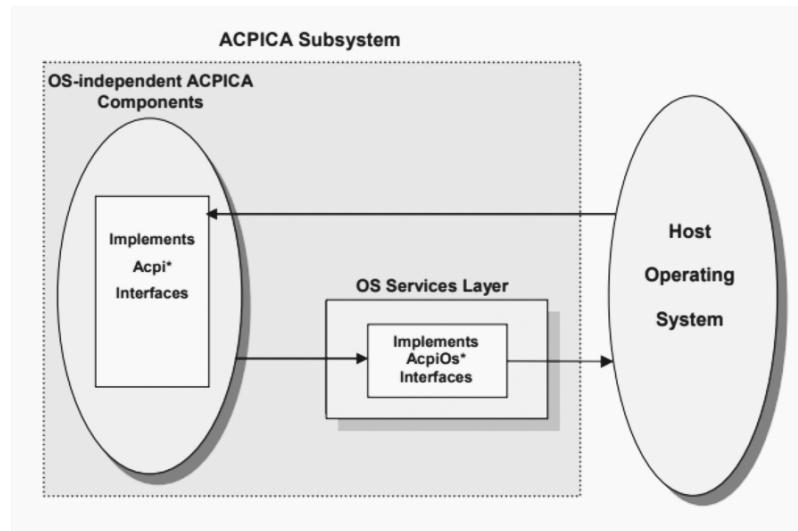


FIGURE 4: Interaction between the Architectural Components

To meet these objectives, the PCI-X 2.0 standard has been developed. PCI-X 2.0 has the performance to feed the most bandwidth-hungry applications while at the same time maintaining complete hardware and software backward compatibility to previous generations of PCI and PCI-X. The PCI-X 2.0 standard introduces two new speed grades: PCI-X 266 and PCI-X 533. These speed grades offer bandwidths that are two times and four times that of PCI-X 133 – ultimately providing bandwidths that are more than 32 times faster than the original version of PCI that was introduced eight years ago. It achieves the additional performance via time-proven DDR (Double Data Rate) and QDR (Quad Data Rate) techniques that transmit data at either 2-times or 4-times the base clock frequency. Because PCI-X 2.0 preserves so many elements from previous generations of PCI it is the beneficiary of a tremendous amount of prior development work. The operating systems, connector, device drivers, form factor, protocols, BIOS, electrical signaling, BFM (bus functional model), and other original PCI elements, are all heavily leveraged in the PCI-X 2.0 specification.

In fact, many of these elements remain identical in PCI-X 2.0. These similarities make implementation easy because these elements have already been designed and engineers are already familiar with them. As a result, the time-to-market is short, and risk is dramatically reduced.

The market migration to PCI-X 2.0 will also be easy because there are so many previous-generation PCI adapter cards already on the market. There are already hundreds of PCI adapter cards that are available today that can be utilized by every PCI-X 266 and PCI-X 533 slot. In addition, new PCI-X 266 and PCI-X 533 adapter cards have ready homes in any of the millions of PCI and PCI-X slots in existing systems. Because of these factors, PCI-X 2.0 provides the ideal next-generation, local I/O solution for high-bandwidth applications. It offers the performance needed for today's and tomorrow's applications in an easy-to-adopt, backward-compatible standard.

1.6.1 Functional Description

PCI BIOS functions provide a software interface to the hardware used to implement a PCI based system. Its primary usage is for generating operations in PCI specific address spaces (configuration space and Special Cycles). PCI BIOS functions are specified to operate in the following modes of the X86 architecture. The modes are: real-mode, 16:16 protected mode (also known as 286 protected mode), 16:32 protected mode (introduced with the 386), and 0:32 protected mode (also known as “flat” mode, wherein all segments start at linear address 0 and span the entire 4-GB address space).

Access to the PCI BIOS functions for 16-bit callers is provided through Interrupt 1Ah. 32-bit (i.e., protected mode) access is provided by calling through a 32-bit protected mode entry point. The PCI BIOS function code is B1h. Specific BIOS functions are invoked using a sub-function code. A user simply sets the host processors registers for the function and sub-function desired and calls the PCI BIOS software. Status is returned using the CARRY FLAG ([CF]) and registers specific to the function invoked.

1.6.2 UEFI PCI Services

UEFI stands for Unified Extensible Firmware Interface. The UEFI Specification, Version 2.3 or later describes an interface between the operating system and the platform firmware. The interface is in the form of data tables that contain platform-related information and boot and run-time services calls that are available to the operating system and its loader. Together, these provide a standard environment for booting an operating system.

The following sections provide an overview of the EFI Services relevant to PCI (including Conventional PCI, PCI-X, and PCI Express). For details, refer to the UEFI Specification. UEFI is processor-agnostic.

1.6.3 UEFI Driver Model

The UEFI Driver Model is designed to support the execution of drivers that run in the pre-boot environment present on systems that implement the UEFI firmware. These drivers may manage and control hardware buses and devices on the platform, or they may provide some software derived platform specific services.

The UEFI Driver Model is designed to extend the UEFI Specification in a way that supports device drivers and bus drivers. It contains information required by UEFI driver writers to design and implement any combination of bus drivers and device drivers that a platform may need to boot an UEFI-compliant operating system.

Applying the UEFI Driver Model to PCI, the UEFI Specification defines the PCI Root Bridge Protocol and the PCI Driver Model and describes how to write PCI bus drivers and PCI devices drivers in the UEFI environment. For details, refer to the UEFI Specification.

- **PCI Root Bridge Protocol** - A PCI Root Bridge is represented in UEFI as a device handle that contains a Device Path Protocol instance and a PCI Root Bridge Protocol instance. PCI Root Bridge Protocol provides an I/O abstraction for a PCI Root Bridge that the host bus can perform. This protocol is used by a PCI Bus Driver to perform PCI Memory, PCI I/O, and PCI Configuration cycles on a PCI Bus. It also provides services to perform different types of bus mastering DMA on a PCI bus. PCI Root Bridge Protocol abstracts device specific code from the system memory map. This allows system designers to make changes to the system memory map without impacting platform independent code that is consuming basic system resources. An example of such system memory map changes is a system that provides non-identity memory mapped I/O (MMIO) mapping between the host processor view and the PCI device view.
- **PCI Driver Model** - The PCI Driver Model is designed to extend the UEFI Driver Model in a way that supports PCI Bus Drivers and PCI Device Drivers. This applies to Conventional PCI, PCI-X, and PCI Express. PCI Bus Drivers manage PCI buses present in a system. The PCI Bus Driver creates child device handles that must contain a Device Path Protocol instance and a PCI I/O Protocol instance. The PCI I/O Protocol is used by the PCI Device Driver to access memory and I/O on a PCI controller. PCI Device Drivers manage PCI controllers present on PCI buses. The PCI Device Drivers produce an I/O abstraction that may be used to boot an UEFI compliant operating system.

1.6.4 Graphics Output Protocol (GOP)

Graphics Output Protocol (GOP) is defined in the UEFI Specification to remove the hardware requirement to support legacy VGA and INT 10h BIOS. GOP provides a software abstraction to draw on the video screen.

1.6.5 BUS Performances and Number of Slots Compared

The various architectures defined by the PCISIG. The table shows the evolution of bus frequencies and bandwidths., as it obvious, increasing bus frequency compromises the number of electrical loads or number of connectors allowable on a bus at that frequencies. At some point for a given bus architecture there is an upper limit beyond which one cannot further increase the bus frequency, hence requiring the definition of a new bus architecture. A PCI express (PCIe) Interconnect that connects two devices is referred to as a Link. A link consists if either x1, x2, x4,

TABLE 2: Comparison of Bus Frequency, Bandwidth and Number of Slots

Bus Type	Clock Frequency	Peak Bandwidth	Number of Card Slots per Bus
PCI 32-bit	33 MHz	133 MBps	4 – 5
PCI 64-bit	33 MHz	266 MBps	4 – 5
PCI 32-bit	66 MHz	266 MBps	1 – 2
PCI 64-bit	66 MHz	533 MBps	1 – 2
PCI-X 32-bit	66 MHz	266 MBps	4
PCI-X 64-bit	66 MHz	533 MBps	4
PCI-X 32-bit	133 MHz	533 MBps	1 – 2
PCI-X 64-bit	133 MHz	1066 MBps	1 – 2
PCI-X 32-bit	266 MHz effective	1066 MBps	1
PCI-X 64-bit	266 MHz effective	2131 MBps	1
PCI-X 32-bit	533 MHz effective	2131 MBps	1
PCI-X 64-bit	533 MHz effective	4262 MBps	1

x8, x12, x16 or x32 signal pairs in each direction. These signals are referred to as Lanes. A designer determines how many Lanes to implement based on the targeted performance benchmark required on a given Link.

The Table 2 shows aggregate bandwidth numbers for various Link width implementations, as is apparent from this table, the peak bandwidth achievable with PCIe is significantly higher than any existing bus today.

1.7 Graphics Controller

Most graphics controllers are PCI controllers. The graphics drivers managing those controllers are also PCI drivers. However, while most graphics controllers are PCI controllers, graphics controllers can make use of other buses, such as USB buses. Graphics drivers have these characteristics:

- UEFI graphics drivers follow the UEFI driver model.
- Depending on the adapter that the driver manages, a graphics driver can be categorized as either a single or a multiple output adapter.
- The graphics driver must create child handles for each output.
- Graphics drivers must create child handles for some of the graphics output ports and attach the Graphics Output Protocol (GOP Protocol), EDID Discovered Protocol, and EDID Active Protocol to each active handle that the driver produced.
- Graphics drivers are chip-specific because of the requirement to initialize and manage the graphics device. A UEFI driver is required for any PC hardware device needed for the boot process to complete. Hardware devices can be categorized into the following:
 - Graphic output devices: Simple text, graphics output.
 - Console devices: Simple input provider, simple input ex, simple pointer — mice, serial I/O protocol (remote consoles)

Note that independent hardware vendors (IHVs) can choose not to implement all of the required elements of the UEFI specification. For example, all elements might not be implemented on a specialized system configuration that does not support all the services and functionality implied by the required elements. Also, some elements are required depending on a specific platform's features. Some elements are required depending on the features that a specific driver requires. Other elements are recommended based on coding experience, for reasons of portability, and/or for other considerations. It is recommended that you implement all required and recommended elements in your drivers.

1.7.1 Graphics Output Protocol

The GOP (Graphics Output Protocol) Driver is part of the UEFI boot time drivers responsible for bringing up the display during bios boot. This driver enables logo display during bios boot time. This paper has a GOP device driver written for an Intel's IoT Android platform which is responsible for display control until the operating system and in turn the display controller of the system gains the control.

1.7.2 GOP Overview

The GOP driver is a replacement for legacy video BIOS and enables the use of UEFI pre-boot firmware without CSM. The GOP driver can be 32-bit, 64-bit, or IA-64 with no binary compatibility. UEFI pre-boot firmware architecture (32/64-bit) must match the GOP driver architecture (32/64-bit). The Intel Embedded Graphics

TABLE 3: Difference between Video BIOS and GOP

Bus Type	Clock Frequency
64 <i>KB</i> limit	execution No 64 <i>KB</i> limit. 32- <i>bit</i> protected mode
CSM is needed with UEFI system firmware	No need for CSM. Speed optimized (fast boot)
16- <i>bit</i> The VBIOS works with both 32- <i>bit</i> and 64- <i>bit</i> architectures	The UEFI pre-boot firmware architecture must match the GOP driver.

Drivers' GOP driver can either be fast boot (speed optimized and platform specific) or generic (platform agnostic for selective platforms).

EFI defines two types of services: boot services and runtime services. Boot services are available only while the firmware owns the platform (i.e., before the ExitBoot-Services call), and they include text and graphical consoles on various devices, and bus, block and file services. Runtime services are still accessible while the operating system is running; they include services such as date, time and NVRAM access. In addition, the Graphics Output Protocol (GOP) provides limited runtime services support. The operating system is permitted to directly write to the frame buffer provided by GOP during runtime mode. However, the ability to change video modes is lost after transitioning to runtime services mode until the OS graphics driver is loaded. This paper includes a GOP driver written for an IoT's platform using the development kit EDK II which is responsible for the display during booting process until the operating system gains control of the display and invoke display devices.

1.7.3 GOP DRIVER

The EFI specification defined a UGA (Universal Graphic Adapter) protocol to support device-independent graphics. UEFI did not include UGA and replaced it with GOP (Graphics Output Protocol), with the explicit goal of removing VGA hardware dependencies. The two are similar.

Table 3 gives a quick comparison of GOP and video BIOS.

1.7.4 GOP Integration

The platform firmware must meet the following requirements for GOP Driver integration:

TABLE 4: GOP Driver files

File Name	Description	Format
GopDriver.efi	The GOP driver binary	Uncompressed PE/COFF image
Vbt.bin	Contains Video BIOS Table (VBT) data	Raw Binary
Vbt.bsf	BMP script file. Required for modifying Vbt.bin using BMP tool	Text

- Platform firmware must be compliant to UEFI 2.1 or later.
- Platform must enumerate and initialize the graphics device.
- Platform must allocate enough graphics frame buffer memory required to support the native mode resolution of the integrated display.
- The platform must produce the standard EFI_PCI_IO_PROTOCOL and as well as the EFI_DEVICE_PATH_PROTOCOL on the graphics device handle. Additionally, the platform must produce PLATFORM_GOP_POLICY_PROTOCOL.
- The platform firmware must not launch the legacy Video BIOS.

The GOP Driver solution comprises the following files shown in Table 4 GOP driver files.

Customize the VBT data file Vbt.bin as per platform requirements and the corresponding BSF file. Integrate Vbt.bin and GopDriver.efi files into the platform firmware image. The process of accomplishing this step is determined by the platform implementer, specific to the platform firmware implementation.

2. Design

2.1 UEFI Design Overview

The design of UEFI is based on the following fundamental elements:

- **Reuse of existing table-based interfaces** - In order to preserve investment in existing infrastructure support code, both in the OS and firmware, a number of existing specifications that are commonly implemented on platforms compatible with supported processor specifications must be implemented on platforms wishing to comply with the UEFI specification.
- **System partition** defines a partition and file system that are designed to allow safe sharing between multiple vendors, and for different purposes. The ability to include a separate, shareable system partition presents an opportunity to increase platform value-add without significantly growing the need for nonvolatile platform memory
- **Boot services** provide interfaces for devices and system functionality that can be used during boot time. Device access is abstracted through "handles" and "protocols". This facilitates reuse of investment in existing BIOS code by keeping underlying implementation requirements out of the specification without burdening the consumer accessing the device.
- **Runtime services** - A minimal set of runtime services is presented to ensure appropriate abstraction of base platform hardware resources that may be needed by the OS during its normal operations.

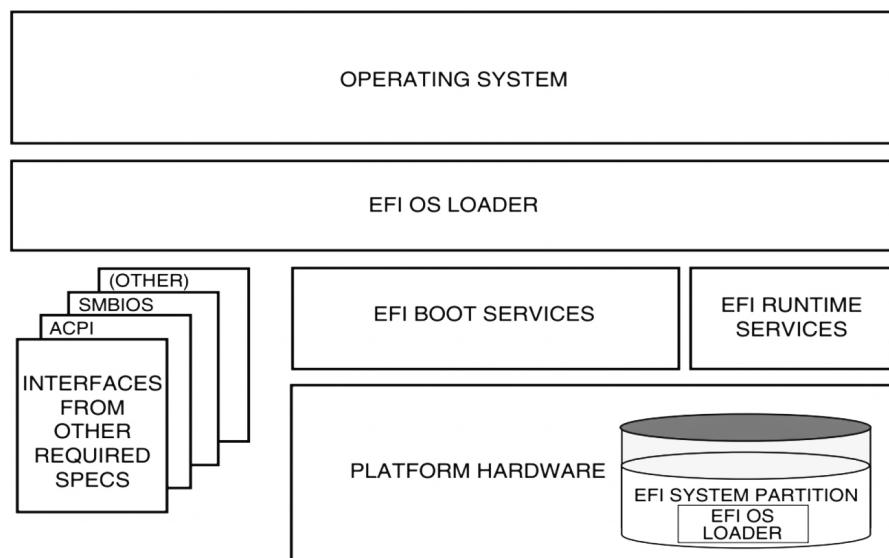


FIGURE 5: UEFI Conceptual Overview

Error! Reference source not found illustrates the interactions of the various components of an UEFI specification-compliant system that are used to accomplish platform and OS boot.

The platform firmware can retrieve the OS loader image from the System Partition. The specification provides for a variety of mass storage device types including disk, CD-ROM, and DVD as well as remote boot via a network. Through the extensible protocol interfaces, it is possible to add other boot media types, although these may require OS loader modifications if they require use of protocols other than those defined in this document.

Once started, the OS loader continues to boot the complete operating system. To do so, it may use the EFI boot services and interfaces defined by this or other required specifications to survey, comprehend, and initialize the various platform components and the OS software that manages them. EFI runtime services are also available to the OS loader during the boot phase.

2.1.1 UEFI Driver Goals

The UEFI Driver Model has the following goals:

- **Compatible** - Drivers conforming to this specification must maintain compatibility with the EFI and the UEFI Specification. This means that the UEFI Driver Model takes advantage of the extensibility mechanisms in the UEFI Specification to add the required functionality.
- **Simple** - Drivers that conform to this specification must be simple to implement and simple to maintain. The UEFI Driver Model must allow a driver writer to concentrate on the specific device for which the driver is being developed. A driver should not be concerned with platform policy or platform management issues. These considerations should be left to the system firmware.
- **Scalable** - The UEFI Driver Model must be able to adapt to all types of platforms. These platforms include embedded systems, mobile, and desktop systems, as well as workstations and servers.
- **Flexible** - The UEFI Driver Model must support the ability to enumerate all the devices, or to enumerate only those devices required to boot the required OS. The minimum device enumeration provides support for more rapid boot capability, and the full device enumeration provides the ability to perform OS installations, system maintenance, or system diagnostics on any boot device present in the system.
- **Extensible** - The UEFI Driver Model must be able to extend to future bus types as they are defined.

- **Portable** - Drivers written to the UEFI Driver Model must be portable between platforms and between supported processor architectures.
- **Interoperable** - Drivers must coexist with other drivers and system firmware and must do so without generating resource conflicts.
- **Describe complex bus hierarchies** - The UEFI Driver Model must be able to describe a variety of bus topologies from very simple single bus platforms to very complex platforms containing many buses of various types.
- **Small driver footprint** - The size of executables produced by the UEFI Driver Model must be minimized to reduce the overall platform cost. While flexibility and extensibility are goals, the additional overhead required to support these must be kept to a minimum to prevent the size of firmware components from becoming unmanageable.
- **Address legacy option rom issues** - The UEFI Driver Model must directly address and solve the constraints and limitations of legacy option ROMs. Specifically, it must be possible to build add-in cards that support both UEFI drivers and legacy option ROMs, where such cards can execute in both legacy BIOS systems and UEFI-conforming platforms, without modifications to the code carried on the card. The solution must provide an evolutionary path to migrate from legacy option ROMs driver to UEFI drivers.

2.2 UEFI/PI Firmware Images

UEFI and PI specifications define the standardized format for EFI firmware storage devices (FLASH or other non-volatile storage) which are abstracted into "Firmware Volumes". Build systems must be capable of processing files to create the file formats described by the UEFI and PI specifications. The tools provided as part of the EDK II BaseTools package process files compiled by third party tools, as well as text and Unicode files in order to create UEFI or PI compliant binary image files. In some instances, where UEFI or PI specifications do not have an applicable input file format, such as the Visual Forms Representation (VFR) files used to create PI compliant IFR content, tools and documentation have been provided that allows the user to write text files that are processed into formats specified by UEFI or PI specifications.

A Firmware Volume (FV) is a file level interface to firmware storage. Multiple FVs may be present in a single FLASH device, or a single FV may span multiple FLASH devices. An FV may be produced to support some other type of storage entirely, such as a disk partition or network device. For more information consult the Platform Initialization Specification, Volume 3. In all cases, an FV is formatted with a binary file system. The file system used is typically the Firmware File System (FFS), but other file systems may be possible in some cases. Hence, all modules are stored as "files" in the FV. Some modules may be "execute in place" (linked at

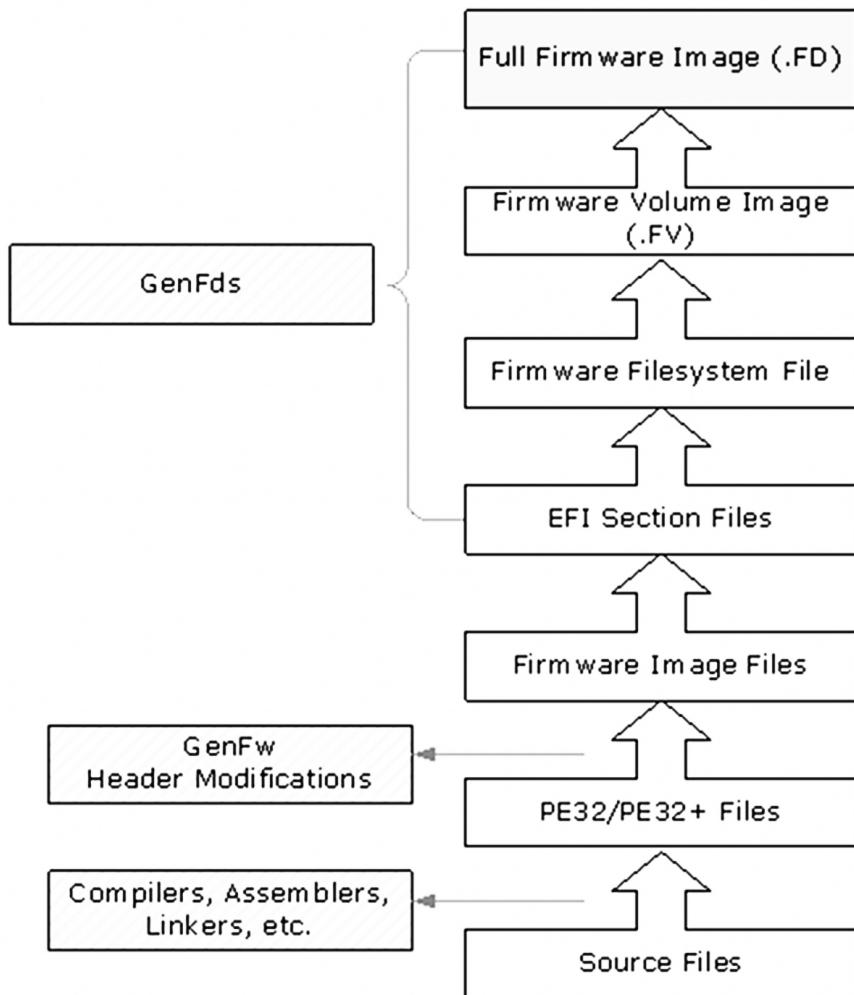


FIGURE 6: UEFI/PI Firmware Image Creation

a fixed address and executed from the ROM), while others are relocated when they are loaded into memory and some modules may be able to run from ROM if memory is not present (at the time of the module load) or run from memory if it is available. Files themselves have an internally defined binary format. This format allows for implementation of security, compression, signing, etc. Within this format, there are one or more "leaf" images. A leaf image could be, for example, a PE32 image for a DXE driver.

Therefore, there are several layers of organization to a full UEFI/PI firmware image. These layers are illustrated below in Figure 6. Each transition between layers implies a processing step that transforms or combines previously processed files into the next higher level. Also shown in Figure 6 are the reference implementation tools that process the files to move them between the different layers.

In addition to creating images that initialize a complete platform, the build process also supports creation of stand-alone UEFI applications (including OS Loaders) and

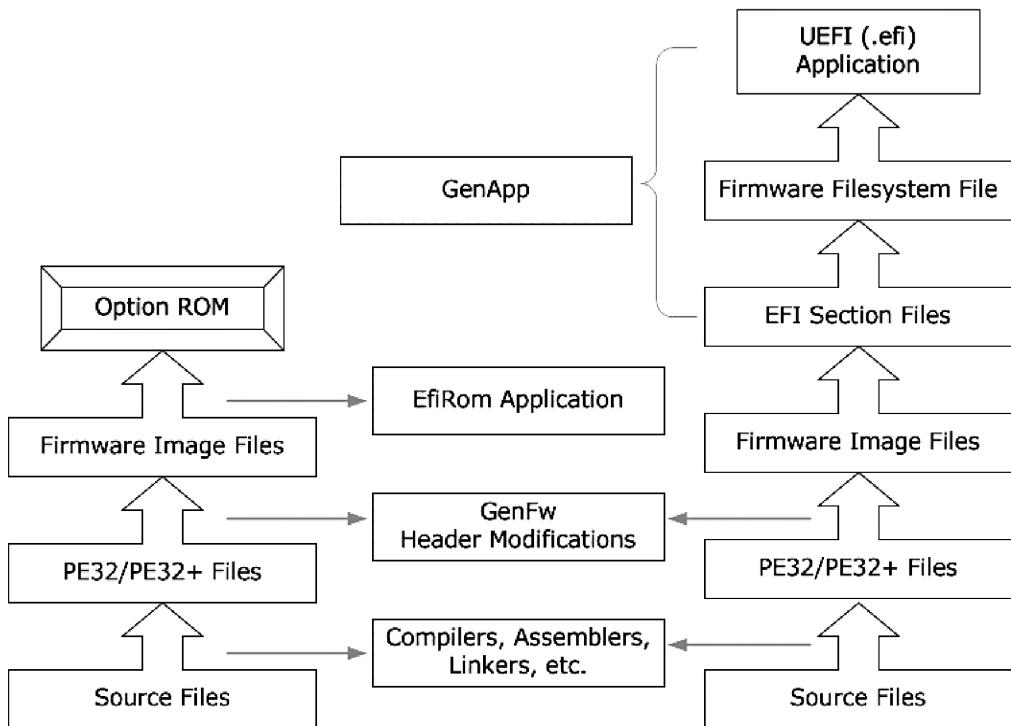


FIGURE 7: UEFI/PI Firmware Image Creation

Option ROM images containing driver code. Figure 7, below, shows the reference implementation tools and creation processes for both of these image types

The final feature that is supported by the EDK II build process is the creation of Binary Modules that can be packaged and distributed for use by other organizations. Binary modules do not require distribution of the source code. This will permit vendors to distribute UEFI images without having to release proprietary source code.

This packaging process permits creation of an archive file containing one or more binary files that are either Firmware Image files or higher (EFI Section files, Firmware File system files, etc.). The build process will permit inserting these binary files into the appropriate level in the build stages.

2.3 Platform Initialization PI Boot Sequence

Platform Initialization PI compliant system firmware has to support the six phases:

1. Security (SEC) Phase
2. Pre-efi Initialization (PEI) Phase
3. Driver Execution Environment (DXE) Phase
4. Boot device selection (BDS) Phase

5. Run time (RT) services and After Life (AL) (transition from the OS back to the firmware) of system.

Figure 8 describes the phases and transition in detail.

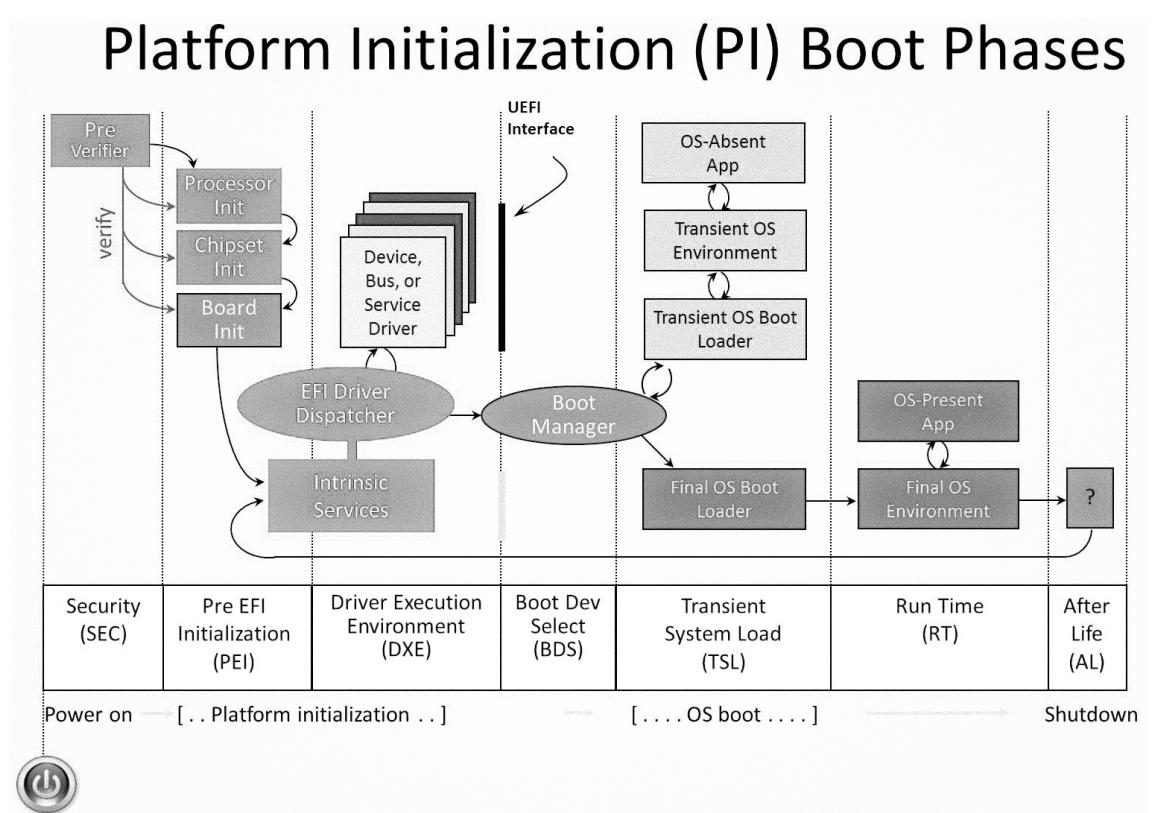


FIGURE 8: PI Boot Phases

2.4 Security (SEC)

The Security (SEC) phase is the initial phase in the PI Architecture and is liable for the following:

- Handling restart events of all platform
- Creation of a temporary memory store
- Bringing the root of trust in the system
- Transit handoff information to next phase - the PEI Foundation

The security section may have the modules with source code scripted in assembly language. Hence, some EDK II module development environment (MDE) modules can consist of assembly code. During Occurrence of this, both Windows and GCC versions of assembly language code are served in different files.

2.5 Pre-EFI Initialization (PEI)

The Pre-EFI Initialization (PEI) phase described in the PI Architecture specifications is invoked quite betimes in the boot period. Specifically, after about preliminary processing in the Security (SEC) phase, any machine restart event will invoke the PEI phase. The PEI phase is designed to be developed in many parts and consists of:

- PEI Foundation (core code)
- Pre-EFI Initialization Modules (specialized plug-ins)

The PEI phase at first operates with the platform in a developing state, holding only on-processor resources, such as the cache of processor for call stack, to dispatch the Pre-EFI Initialization Modules (PEIMs).

The PEI phase cannot assume the availability of amounts of memory (RAM) as DXE and hence PEI phase limits its support to the following:

- Locating and validating PEIMs
- Dispatching PEIMs
- Facilitating communication between PEIMs
- Providing handoff data to later phases

These PEIMs are responsible for the following:

- Initializing some permanent memory complement
- Characterizing the memory in Hand-Off Blocks (HOBs)
- Characterizing the firmware volume locations in HOBs
- Transit the control into next phase - the Driver Execution Environment (DXE) phase

Figure 9 shows a diagram describes the action carried out during the PEI phase

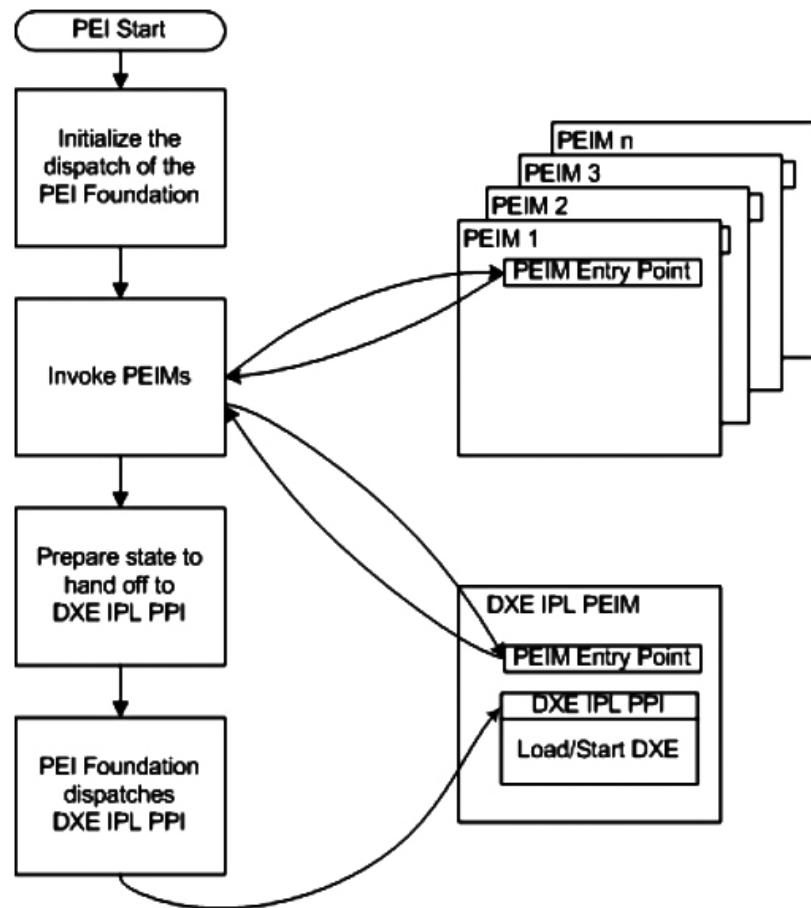


FIGURE 9: Diagram of PI Operations

2.5.1 PEI Services

The PEI Foundation institutes a system table for the PEI Services named as PEI Services Table that is viewable to all PEI Modules (PEIMs) in the system. A PEI Service is defined as a method, command or other potentiality manifested by the PEI Foundation when that service's initialization needs are met. As the PEI phase having no permanent memory available until almost the end of the phase, all the various types of services created during this phase (PEI phase) cannot be as enrich as those created during later phases. A pointer to PEI Services Table is sent into entry point of each PEIM's and also to part of each PEIM-to-PEIM Interface (PPI) because the location of PEI Foundation and its temporary memory is unknown at build time.

The PEI Foundation provides the classes of services listed in Table 5

2.5.2 PEI Foundation

The PEI Foundation is the entity that carried outs following activity:

TABLE 5: Services provided by PEI Foundation Classes

Service	Details
PPI Services	Manages PPIs to ease inter-module method calls between PEIMs. A database maintained in temporary RAM to track installed interfaces.
Boot Mode Services	Manages the boot mode (S3, S5, diagnostics, normal boot, etc.)
HOB Services	Creates data structures (Hand-off-blocks) that are used to convey information to the next phase
Firmware Volume Services	Finds PEIMs and along with that other firmware files in the firmware volumes
PEI Memory Services	provides a collection of memory management services (to be used before and after permanent memory is discovered)
Status Code Services	Provides general progress and error code reporting services (i.e. port 080h or a serial port for text output for debug)
Reset Services	Provides a common means to aid initializing warm or cold restart of the system

- Dispatching of Pre-EFI initialization modules (PEIMs)
- Maintaining the boot mode
- Initialization of permanent memory
- Invoking the DXE loader

The PEI Foundation written to be portable across all the various platforms architecture of a given instruction-set. i.e. A binary for IA-32 (32-bit Intel architecture) works across all Pentium processors and similarly Itanium processor family work across all Itanium processors.

Irrespective of the processor micro architecture, the set of services uncovered by the PEI Foundation should be the same. This consistent surface area around the PEI Foundation allows PEIMs to be written in the C programming language and compiled across any micro architecture.

2.6 PEI Dispatcher

The PEI Dispatcher is basically a state machine which is implemented in the PEI Foundation. The PEI Dispatcher evaluates the dependency expressions in Pre-EFI initialization modules (PEIMs) that are lying in the FVs being examined.

Dependency expressions are coherent combinations of PEIM-to-PEIM Interfaces (PPIs). These expressions distinguish the PPIs that must be available for use before a given PEIM can be invoked. The PEI Dispatcher references the PPI database in the PEI Foundation to conclude which PPIs have to be installed and evaluate the dependency expression for the PEIM. If PPI has already been installed then dependency expression will evaluate to TRUE, which notifies PEI Dispatcher it can run PEIM. At this stage, the PEI Foundation handovers control to the PEIM with TRUE dependency expression.

The PEI Dispatcher will exit Once the PEI Dispatcher has examined and evaluated all of the PEIMs in all of the uncovered firmware volumes and no more PEIMs can be dispatched (i.e. the dependency expressions (DEPEX) do not evaluate from FALSE to TRUE). At this stage, the PEI Dispatcher cannot invoke any additional PEIMs. The PEI Foundation then takes back control from the PEI Dispatcher and calls the DXE IPL PPI to navigate control to the DXE phase of execution.

2.7 Drive Execution Environment (DXE)

Before the DXE phase, the Pre-EFI Initialization (PEI) phase is held responsible for initializing permanent memory in the platform. Hence, DXE phase can be loaded and executed. At the very end of the PEI phase, state of the system is handed over to the DXE phase through Hand-Off Blocks (list of position independent data structures).

There are three components in the DXE phase:

1. DXE Foundation
2. DXE Dispatcher
3. A set of DXE Drivers

2.8 Boot Device Selection (BDS)

The BDS Architectural Protocol has part of implementation of the Boot Device Selection (BDS) phase. After evaluation of all of the DXE drivers dependencies, DXE drivers with satisfied dependencies are loaded and executed by the DXE Dispatcher, the DXE Foundation will pass the control to the BDS Architectural Protocol. The BDS phase held responsible for the following:

- Initializing console devices
- Loading device drivers
- Attempt of loading and executing boot selections

2.9 Transient System Load (TSL) and Runtime (RT)

Primarily the OS vendor provides boot loader known as The Transient System Load (TSL). TSL and Runtime Services (RT) phases may allow access to persistent content, via UEFI drivers and applications. Drivers in this category include PCI Option ROMs.

2.10 After Life (AL)

The After Life (AL) phase contains the persistent UEFI drivers used to store the state of the system during the OS systematically shutdown, sleep, hibernate or restart processes.

2.11 Generic Build Process

All code initialized as either C sources and header files, assembly language sources and header files, Unicode files (UCS-2 HII strings), Virtual Forms Representation files or binary data (native instructions, such as microcode) files. Per the UEFI and PI specifications, the C files and Assembly files must be compiled and coupled into PE32 or PE32+ images. While some code is configured to execute only from ROM, most UEFI and PI modules code are written to be relocatable. These are written and built different i.e. XIP (Execute In Place) module code is written and compiled to run from ROM, while the majority of the code is written and compiled to execute from memory, which needs the relocatable code.

Some modules may also allow dual mode, where it will execute from memory only if memory is sufficient, otherwise it will execute from ROM. Additionally, modules may permit dual access, such as a driver that contains both PEI and DXE implementation code. Code is assembled or compiled, then linked into PE32/PE32+ images, the relocation section may or may not be stripped and an appropriate header will replace the PE32/PE32+ header. Additional processing may remove more non-essential information, generating a Terse (TE) image. The binary executables are converted into EFI firmware file sections. Each module is converted into an EFI Section consisting of an Section header followed by the section data (driver binary).

2.11.1 EFI Section Files

The general section format for sections less than 16MB in size is shown in Figure 11. Figure 10 shows the section format for sections 16MB or larger in size using the extended length field.

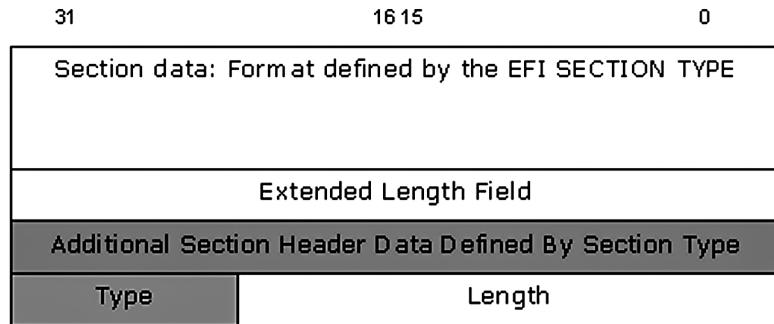


FIGURE 10: General EFI Section Format for large size Sections(greater than 16 MB)

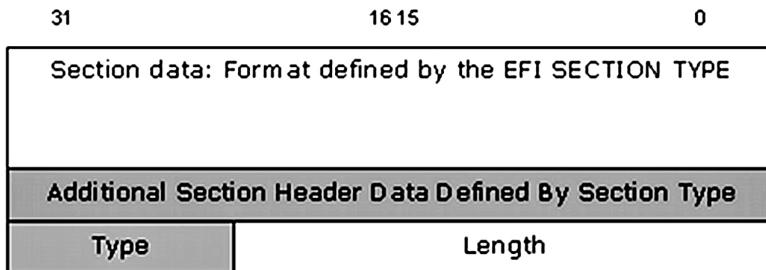


FIGURE 11: General EFI Section Format (less than 16 MB)

2.12 Cross Compatibility of CPUs

Whenever customer try to change the default Intel motherboard CPU with different Intel silicon chip which won't work. The specific CPU Chip initialization varies for each generation. So, the board designs should be designed in such a way that specific generation CPU should support., if we change the CPU with a different Intel Board it will not even boot, because the BIOS doesn't support for other Silicon Initialization for other CPUs.

So, we are integrating the runtime detection of the silicon during the Pre-Extensible Firmware Initialization (PEI) phase. So, within single Integrated Firmware Image (IFWI) should support the Multi Generation CPUs which is never tried before.

Each silicon has a fixed register from which the CPU generation can be identified., so the BIOS should read that register and program in such a way the is CPU1 is in Platform it should support the CPU1 Features like PCIe, Graphics & DMI., if the

CPU1 is replaced with CPU2 then it should support the CPU2 speed. That should be taken care by the BIOS.

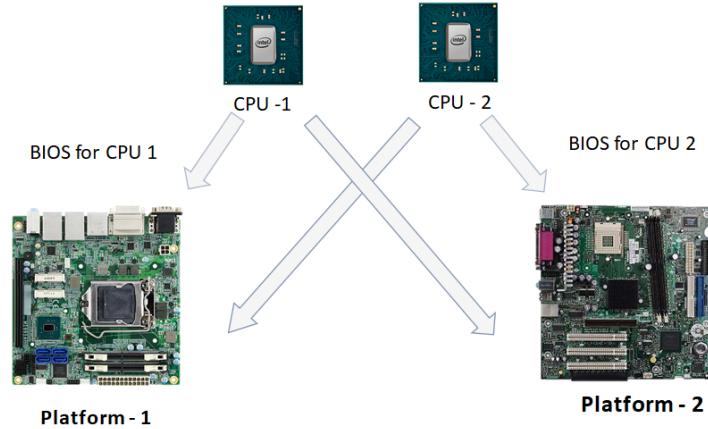


FIGURE 12: Cross Compatibility Design

Figure 12 shows the general view of the Cross Compatibility of CPUs.

BIOS is the part of Integrated Firmware Image which resides at the End of the Binary table. The CPU swap can only occur in Specially designed Intel Designed Board only. Mainly because for each and every feature it required some hardware(H/W) requirements. If that H/W requirement not present. Then It will boot but doesn't support the Maximum speed.

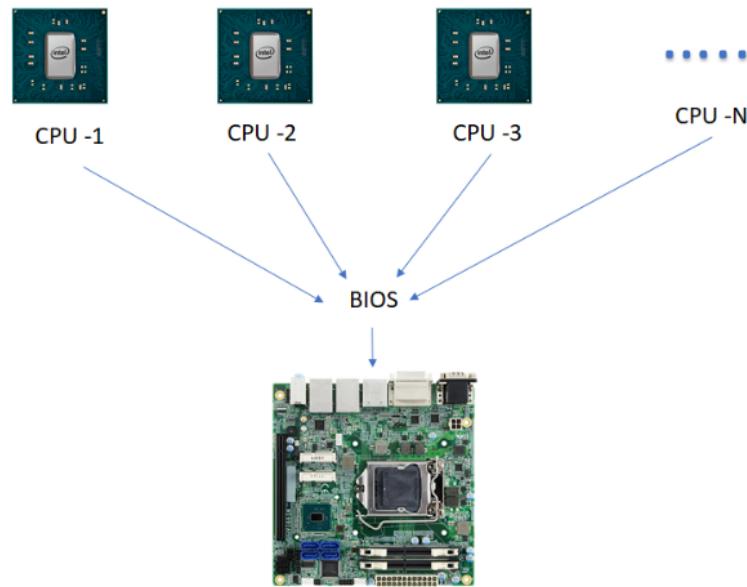


FIGURE 13: BIOS Support for Cross Compatibility

Figure 13 shows the BIOS role for identifying the CPUs during PEI phase.

As the number of Feature increases in the Silicon BIOS size also increases, usually the BIOS size varies from Platform to Platform and CPU to CPU., as we are integrating the Compatibility the BIOS size obviously increases.

The structure of IFWI is Shown in Figure 14

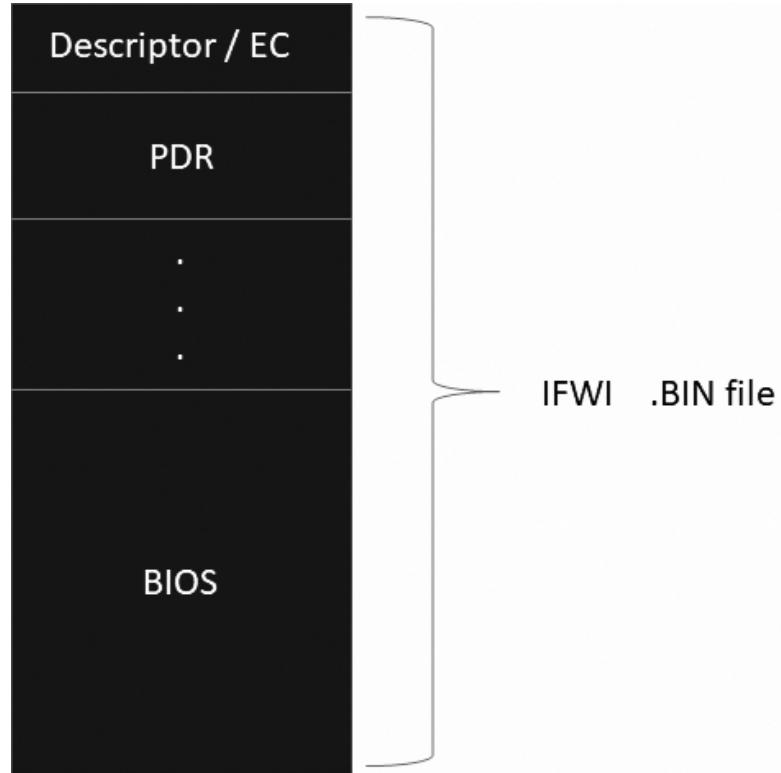


FIGURE 14: Integrated Firmware Image

3. Architecture of BIOS Firmware

3.1 Overview

If you interpret BIOS image as close look then it is nothing but the file system which is made in a byte format to be read by low level programming language which is most efficient method to store the data or content.

The concept of initialization of Platform includes the execution of this BIOS image which is stored on the every SoC

The components which plays role in Platform Initialization are listed below:

- Firmware Volume (FV) - consists of one or more firmware file systems
- Firmware File System (FFS) which consists of one or more firmware files
- Firmware File - Encapsulated section or leaf section
- Reference Layout of Binary
- Pre-EFI Initialization (PEI) PEIM to PEIM Interfaces (PPIs)
- Driver Execution Environment (DXE) Protocols

3.2 Design of Firmware Storage

Design of firmware storage elaborates the way that how files needs to be stored and accessed in nonvolatile storage environment. Implementation of any firmware has to support and follow the standard structure for PI Firmware Volume and the structure of FFS.

Firmware Device - a persistent physical repository consisting data and/or firmware code. Typically it is a component of flash but may also be any other type of persistent storage. Singular physical firmware device can be partitioned in to multiple other smaller pieces to form many other logical firmware devices from it and vice-versa.

Flash devices are most usual nonvolatile storage mechanism for firmware volumes. Often, flash devices are partitioned into many sectors or blocks of potentially differing sizes, each along with various runtime characteristics.

In the design of Firmware File System (FFS), several observed unique qualities of flash devices are listed below:

- Erase operation processed on the basis of sector-by-sector. After ensuring, every bits of sector return their erase value¹.
- Write operation can be performed on a bit-by-bit basis. i.e. In case erase value is 0 then bit value 0 can be changed to 1.
- Only by performing erase operation on the whole flash sector, non-erase value can change to erase value.
- Capable of enable/disable reads and writes to individual flash sectors or the entire flash.
- Operations like writes and erases are much longer than reads operation.
- Many times places restraints on the trading operations that can be executed while a write or erase is in progress.

3.3 Firmware Volume (FV)

The BIOS image is consisting of one or more logical firmware devices known as a Firmware Volume (FV). Firmware Volume is the very basic and efficient logical storage mechanism for data and/or code. If you consider file system as a basic unit then firmware volume is unionized into these one or more file system units. Table 6 describes attributes in each firmware volume.

Apart from this Firmware volumes also consisting of few more information about the correspondence between OEM file types and a GUID.

3.4 Firmware File System (FFS)

The logical data payload within firmware volume is known as a Firmware File System (FFS) which illustrates the structure of files and free space (if any). To affiliate a driver to firmware volume every firmware file systems contains a globally unique ID (GUID).

Firmware files consists of code or raw data or both. Attributes of files are described in Table 7.

Integrity check and staged file creation are some extra attribute formats which might spotted in some firmware volume. Firmware File Sections are unit which unionized in a standard fashion to form certain file types for the file data.

OEM file types (described in detail in Figure 15) enables to support non-standard file types.

¹either all 0 or all 1

TABLE 6: Firmware Volume Attributes

Attribute	Description
Name	each volume has a unique identifier name having UEFI Globally Unique Identifier (GUID).
Size	describes total size of all data (includes all information like headers, files and free/reserved space)
Format	describes type of Firmware File System (FFS) which is unionized in construction of the volume.
Memory is Mapped or not?	some volumes may require to be memory-mapped which determines whether the entire content of the volume can appear at once in the processor's memory address space.
Sticky Write?	Specifies whether or not special erase cycles are required in order to change value of bits into an erase value from non-erase value
Erase Polarity	In case a volume supports <i>Sticky Write</i> , then after processing an erase cycle every bits in the volume will return to this value (0 or 1)
Alignment	A volume is required to be aligned on some power-of-two (2^x) boundary such that <i>minimum</i> \geq highest file alignment value.
Enable/Disable Read capable status	Decides whether to keep volumes as hidden from readable or not
Enable/Disable Write capable Status	Decides whether to keep volumes as hidden from writable or not
Lock Capable/Status	Volumes could also have their locking mechanism
Read-Lock Capable/Status	Volumes could also have the power to lock their read status
Write-Lock Capable/Status	Volumes could also have the power to lock their write status

TABLE 7: Firmware Files Attributes

Attribute	Description
Name	each volume has a unique identifier name having UEFI Globally Unique Identifier (GUID). Name of the File(s) has to be unique within a same firmware volume.
Type	Type of the individual file which can be Normal, OEM, Debug, FV Specific. More file types information are described in Figure 15.
Alignment	Every data of file to be aligned on some power-of-two (2^x) boundary such that these boundaries are founded depending on the alignment of firmware volume.
Size	Describes size of each file which consists of data of size zero or more bytes

PEI phase is responsible to serve the file related services which are carried out using PEI Service Table. On the Other hand the `EFI_FIRMWARE_VOLUME2_PROTOCOL` services which are attached to a volume's handle (`ReadFile`, `ReadSection`, `WriteFile` and `GetNextFile`) are responsible to carried out file related services in DXE phase.

3.4.1 Firmware File Types

If you consider an application with file name such as `XYZ.exe`, in which content format of `XYZ.exe` is implied by the ".exe" in the file name. Based on the situation of operation, this extension normally signals the contents of `XYZ.exe`. The PI Firmware File System characterizes the contents of a file that is returned by the firmware volume interface.

Firmware File System of the Platform Initialization dictates an enumeration of many file types. For example, the type `EFI_FV_FILETYPE_RAW` implies that the file is a RAW Binary Data. In the same way, files with the type `EFI_FV_FILETYPE_SMM_CORE` supports MM traditional mode .

3.5 Firmware File Section

Firmware File Section is individual distinct unit of certain file types which has following attributes:

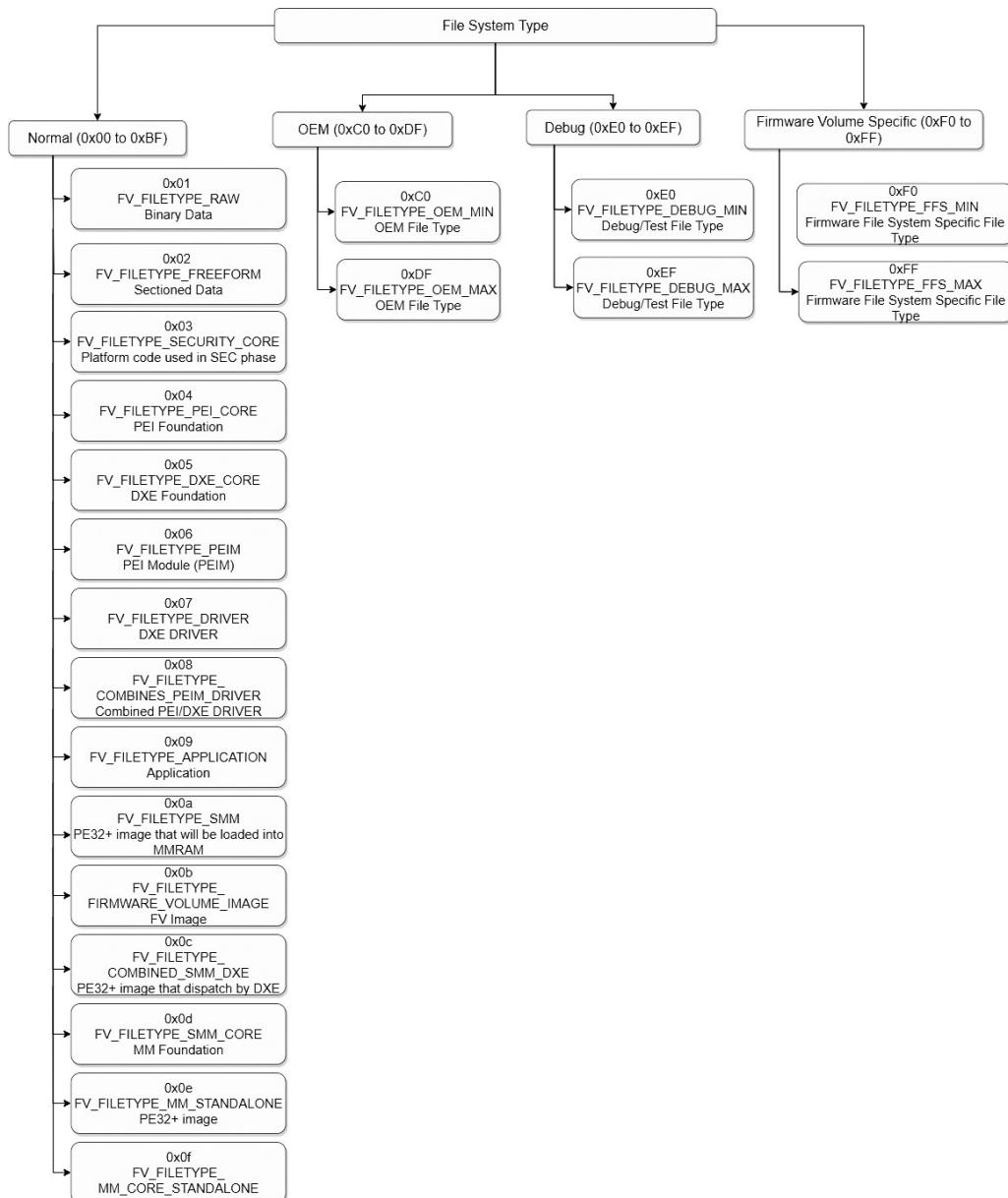


FIGURE 15: Firmware File Type

Attribute	Description
Type	Each section has type
Size	describes size of the section

However as many as types of sections are present, they eventually fall in one of the below broadly described categories:

- **Encapsulation section** - logical storage consisting of the one or more section. The child section(s) which are lying within the encapsulation section (parent section) can be another encapsulation section or a leaf section which are also called relative peers to each other. An encapsulation section never consists of data in itself; however it is just a container that ultimately ends in leaf section(s). Files which are stacked with section can be imagined as tree consisting of nodes (encapsulation section) and leaves (leaf section). The root which can be interpreted as the file image itself may have a discrete number of sections. Sections that exist in the root have no parent section but are still considered peers.
- **Leaf Sections** - Contrary to the encapsulation section, leaf section does contain data and only data within it. Type of section defines which kind of data is stored within the leaf section.

As illustrated in Figure 16, the root which we interpret as the file image has two encapsulation sections which are $E0$, $E1$ and one leaf section which is $L3$. $E0$ which is the first encapsulation section possessing three child node which are all leaves ($L0$, $L1$, and $L2$). $E1$ is the another encapsulation section which possesses only two children, where one of them is encapsulation ($E2$) and the another is the leaf ($L6$). $E2$ which is the very last encapsulation section consists two children which are both leaves only ($L4$ and $L5$).

With the help of `FfsFindSectionData`, services related to section are populated with the help of PEI Service Table in the PEI phase. On the other hand `ReadSection` which is attached to service protocol `EFI_FIRMWARE_VOLUME2_PROTOCOL` responsible to populate services related to section during the DXE phase.

3.6 Firmware File Section Types

Subjective types of section are described in Table 8.

3.7 PI Architecture Firmware File System Format

Basic encoding of binary used for PI firmware file, firmware volume and file system is illustrated in this section. Development which carries out the non-vendor firmware files or firmware volumes to be enclosed into the system must have the standard formats. These sections also describes the way features of the standard format mapped into the standard interfaces of DXE and PEI.

TABLE 8: Types of Section

Name of Section	Value	Details
EFI_SECTION_COMPRESSION	0x1	non-leaf section containing compressed section(s) within
EFI_SECTION_GUID_DEFINED	0x2	non-leaf section which only to be used while in process of build and not for execution
EFI_SECTION_DISPOSABLE	0x3	non-leaf section which only to be used while in process of build and not for execution
EFI_SECTION_PE32	0x10	Image executable of PE32+
EFI_SECTION_PIC	0x11	Code independent of position
EFI_SECTION_TE	0x12	Image of Terse Executable
EFI_SECTION_DXE_DEPEX	0x13	Expression for DXE driver dependency
EFI_SECTION_VERSION	0x14	version of the section - text/numeric
EFI_SECTION_USER_INTERFACE	0x15	Human readable and easily interpretable name for driver
EFI_SECTION_COMPATIBILITY16	0x16	16-bit exe of DOS fashion
EFI_SECTION_FIRMWARE_VOLUME_IMAGE	0x17	PI Firmware Volume Image
EFI_SECTION_FREEFORM_SUBTYPE_GUID	0x18	Raw data with GUID in header to define format
EFI_SECTION_RAW	0x19	Raw data
EFI_SECTION_PEI_DEPEX	0x1b	Expression for PEI driver dependency
EFI_SECTION_SMM_DEPEX	0x1c	Leaf section which determine the order of dispatch for the MM Traditional driver in SMM.

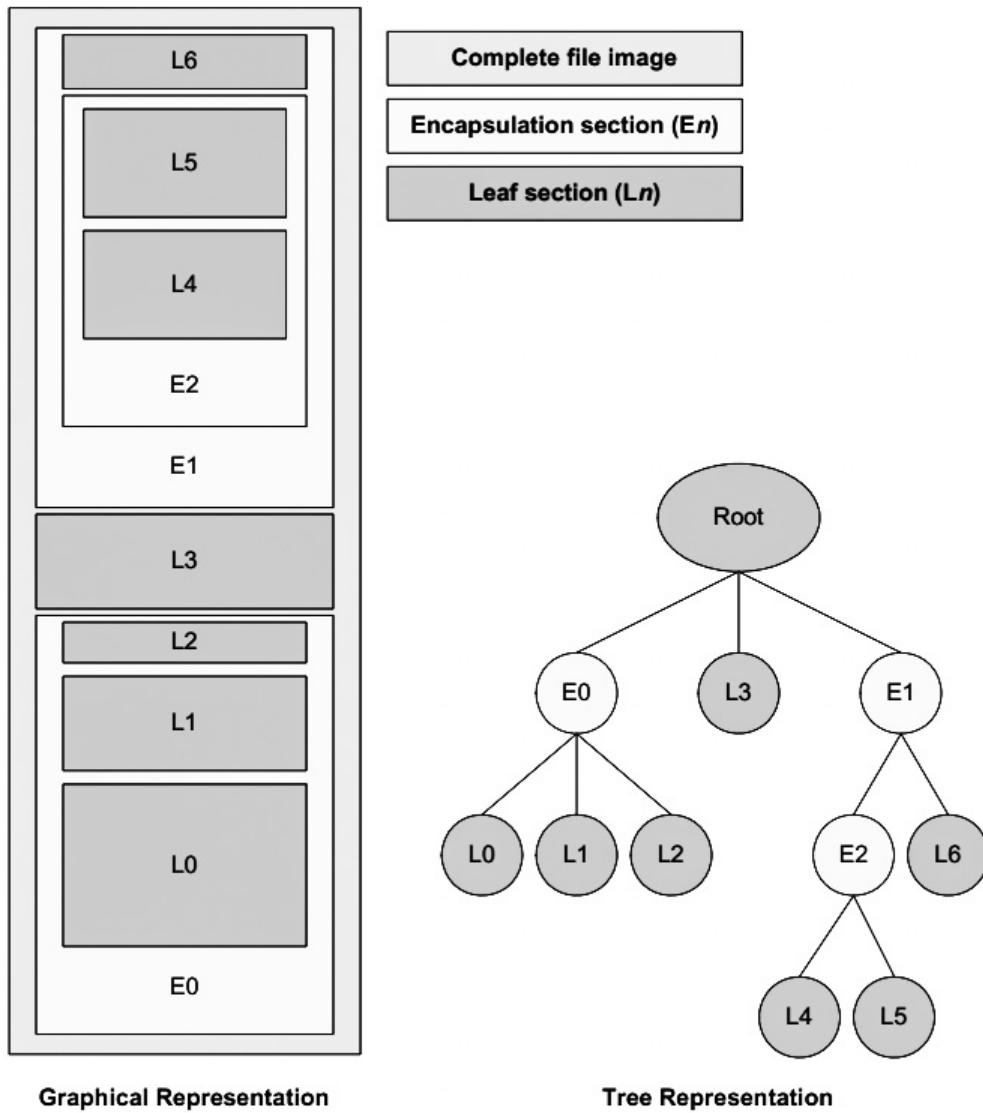


FIGURE 16: Example File System Image

The standard format of firmware file and volume also brings in extra dimensions and potential that are used to assure the unity of firmware volume. The standard format is unionized by three different levels: firmware volume, firmware file system, and firmware file.

The guided formatting of firmware volume (Figure 17) made of two parts: The FV header and FV data. Header of FV describes every attributes mentioned in “Firmware Volumes” in Table 6. This header also has GUID which identifies format of the firmware file system utilized to orchestrate data in the firmware volume. The “firmware volume header” is compatible with every other firmware file systems except the PI Firmware File System.

“Firmware File System format” explains the way the firmware files and free space are conceived inside the firmware volume. However on the other hand “Firmware

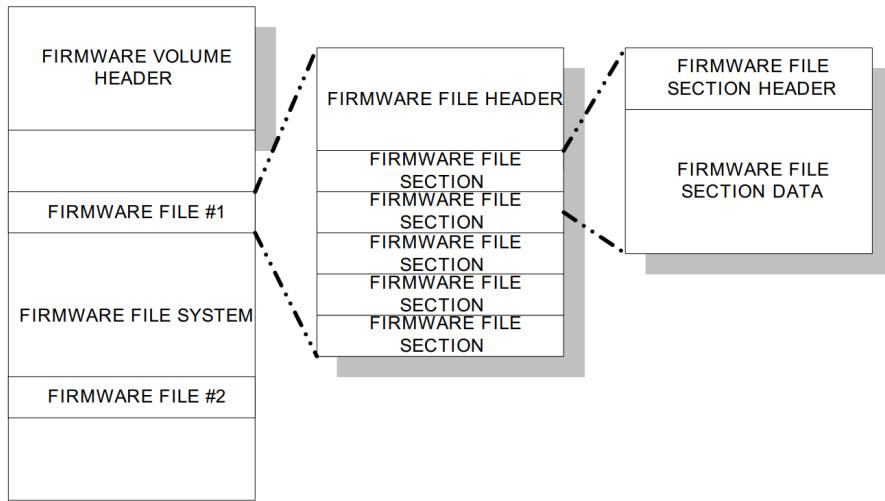


FIGURE 17: The Firmware Volume Format

File format” describes how files are organized. The firmware file format made of two parts: the firmware file header and the firmware file data.

3.7.1 Firmware Volume Format

The PI Architecture Firmware Volume format key outs the binary structure of a firmware volume. The firmware volume format possesses a FV header followed by the FV data. The FV header is represented by variable `EFI_FIRMWARE_VOLUME_HEADER`. The format layout of the FV data is described by a GUID. Valid files system GUID values are `EFI_FIRMWARE_FILE_SYSTEM2_GUID` and `EFI_FIRMWARE_FILE_SYSTEM3_GUID`.

3.7.2 Firmware File System Format

The PI Architecture Firmware File System is a binary design of logical file storage within firmware volumes. It is a flat file system in which there is no rendering of any directory hierarchy structure. Each and every files lies directly in the root of the storage. Files are stored end to end without any directory entry to explain which files are present. Parsing the information stored in a firmware volume to find a itemization of files exists needs the complete walk through over the firmware volume in and out.

Firmware File System GUID The firmware volume header has a unique data field for the file system GUID. The two valid FFS file systems are defined by the GUID values in variable `EFI_FIRMWARE_FILE_SYSTEM2_GUID` and `EFI_FIRMWARE_FILE_SYSTEM3_GUID`. In case of the FFS file system, if it does allows files larger than 16 *MB* along with backward compatibility `EFI_FIRMWARE_FILE_SYSTEM2_GUID` then `EFI_FIRMWARE_FILE_SYSTEM3_GUID` is used.

Volume Top File known as VTF is a file that has to be presented such that the very last byte of file is also the very last byte of the firmware volume. Irrespective of type of the file, a VTF have to have GUID for the file name which is declared as variable `EFI_FFS_VOLUME_TOP_FILE_GUID`. Driver code if Firmware file system has to be exposed of this GUID and infix an alignment pad file as and when needed to assure that the VTF is situated correctly at the top of the firmware volume. Length and alignment of File requirements needs to be coherent with the top of volume so that a write error does occurs and the unwanted firmware volume modification can be prevented.

3.8 Firmware File Format (FFS)

Every FFS files begins with its header data that is aligned on an $8 - byte$ (which is power-of-two 2^3) boundary with respect to the origin of the firmware volume. FFS files consists of the below parts:

- Header
- Data

When a zero-length file is created without any data it still has to have header and will consume minimum $24 bytes$ of space.

The data (if any) exists in file then it immediately conjugated after the header. How the data within a file is formed can be identified by the “Type” field in the header which can be either of `EFI_FFS_FILE_HEADER` and `EFI_FFS_FILE_HEADER2`.

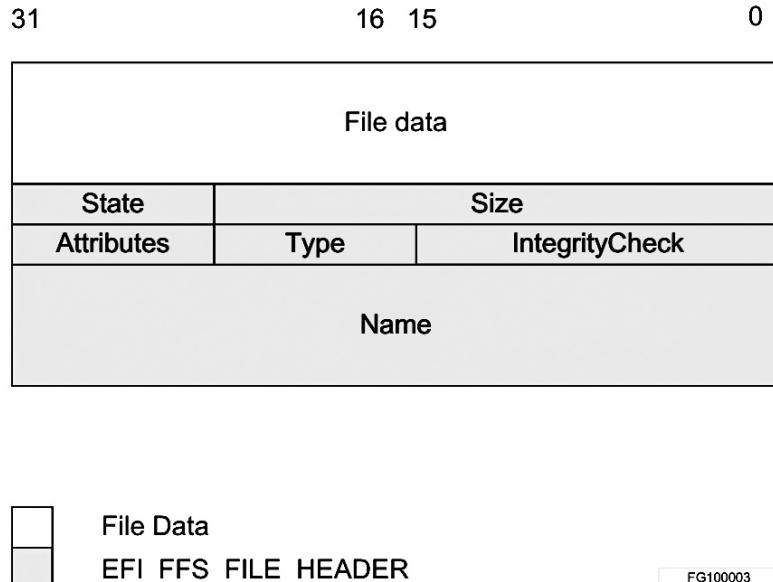
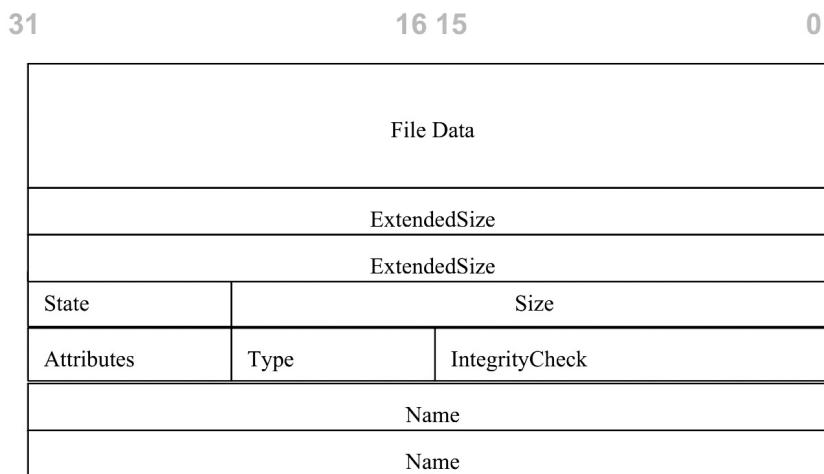
Figure 18 exemplifies the typical layout of a (i.e. `EFI_FFS_FILE_HEADER`) “PI Architecture Firmware File” ($\leq 16Mb$).

Figure 19 exemplifies the typical layout of “PI Architecture Firmware File” ($> 16Mb$).

3.9 Firmware File Section Format

Storage Data format mechanism of section is described in this section. Each individual section starts with a section header which is followed by the data defined using the section type. Section headers are always aligned at $4 - byte$ boundaries with respect to the start of the file image. In case of padding required between the section then to achieve the $4 - byte$ alignment as defined, every bit value of padding is set to zero. There some section types which are variable in terms of data length and are more precisely represented as data streams instead of data structures.

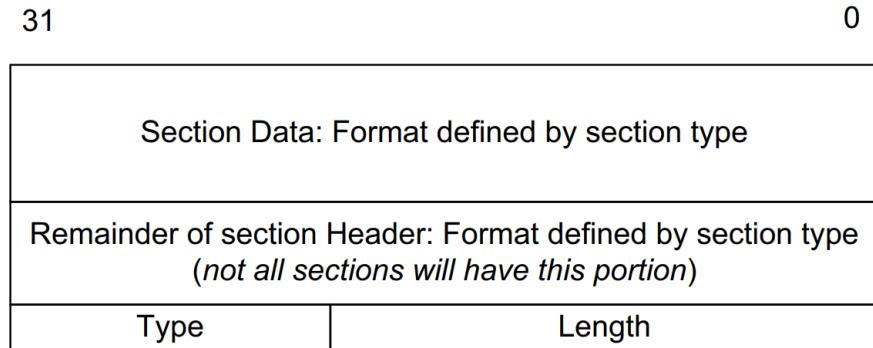
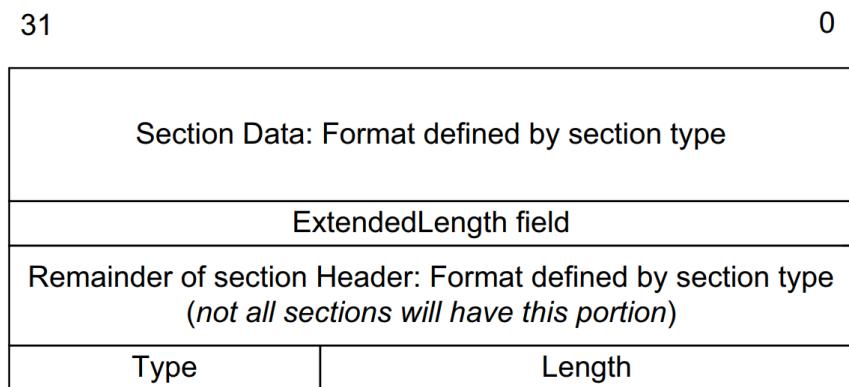
Irrespective of type of the section, all section headers starts with a $24 - bit$ integer telling the section size, and $8 - bit$ section type. The format of the rest of the

FIGURE 18: Layout representation of FFS File Header ($\leq 16Mb$)FIGURE 19: Layout representation of FFS File Header 2 layout for files ($> 16Mb$)

section header and data is defined by the section type. If size of the section size is `0xFFFFFFF` then the size is defined by a *32-bit* integer that follows the *32-bit* section header. Figure 20 and Figure 21 shows the typical layout of a section data format.

3.10 File System Initialization

To ensure unity of the file system it is mandatory to maintain state byte of each file correctly such that it won't compromised even in case of power failure during operation on any FFS. It is desired that an FFS driver produces an instance of

FIGURE 20: Section Header Format when $size < 16Mb$ FIGURE 21: Section Header Format of when $size \geq 16Mb$ using Extended Length field

Firmware Volume Protocol so that every normal file operations carried out in that context. Every file operations has to follow all the rules of creation, update, and deletion mentioned in this specification to avoid corruption of the file system.

3.11 Traversal and Access to Files

The Security (SEC), PEI, and early DXE code needs to be capable to traverse the FFS such that it's read and execute operation on files carried out before a write-enabled DXE FFS driver is started its execution so that the FFS may not have any inconsistencies because of any kind of previous system failure. Hence, it has to follow a set of rules to assert the credibility of files before using them. It is not incumbent on SEC, PEI, or the early read-only DXE FFS services to make any effort to perform recovery or modification the file system. If any case exists where execution can not continue because of inconsistencies in file system, a recovery boot must be initiated.

As there is one mutual exclusiveness that the SEC, PEI, and early DXE code can affect without instantiating a recovery boot. This condition can be summoned by

any previous system failure such as power failure that come along while a file update on a previous boot. In such case, a failure can cause two files with an identical file name GUID to coexist within the same firmware volume where one of them will have the EFI_FILE_MARKED_FOR_UPDATE bit set to its state field but are going to be otherwise totally valid file. The another file may be in unknown state of building up to and including EFI_FILE_DATA_VALID. All files used preceding to the initialization of the write-enabled DXE FFS driver must be filtered with this test prior to their use. If this condition is observed, it's tolerable to trigger a recovery boot and allow the recovery DXE to perform the completion of update.

Note There's no ascertain for redundant files once a file found in the EFI_FILE_DATA_VALID state. The condition where two files in same firmware volume coexist having the same file name GUID and both are within the EFI_FILE_DATA_VALID state cannot occur if the set of rules for creation and update are strictly followed.

3.12 File Integrity and State

File corruption, no matter the cause, must be detectable in order to carried out appropriate steps for file system repair. File corruption can come from various sources but broadly falls into three categories listed below:

- Any general failure
- Failure on erase
- Failure on write

A general failure is characterized to be evidently random corruption of the storage media. This corruption can occur because of the design problem or obsolete storage media i.e. This type of failure can be as perceptive as replacing any single bit inside the file content. Using a good design of system along with reliable storage media, general failures can be avoided. However, the FFS enables catching of this kind of failure.

An erase failure happens when a block erase of firmware volume media isn't completed because of any system failure i.e. power failure. As the erase operation is not outlined, it is likely that most of the implementation of FFS that allow file write and delete operations will also develop a mechanism to rectify deleted files and unite free space. In case the operation is not carried out successfully, the file system can be left out in a state which is not consistent.

Likewise, a write failure takes place when a file system write is in motion and is left incomplete because of any system failure i.e. power failure. This type of failure can lead the file system to be in an inconsistent state.

All of these failures can be traced while FFS initialization is in progress hence depending on the cause of the failure, many recovery schemes can be carried out.

4. System Management Mode (SMM)

4.1 Overview

On IA-32 processors, System Management Mode (SMM) is a manner of operation which is different from flat modal so as from protected mode of the DXE and PEI phases. It is outlined as a real mode environs with $32-bit$ data bus access and its carried out in effect to either with a specified interrupt type or with the System Management Interrupt (SMI) pin. Note that Operation mode of SMM is OS independent mode and is discrete operational mode, however it may also lies in both within and OS runtime.

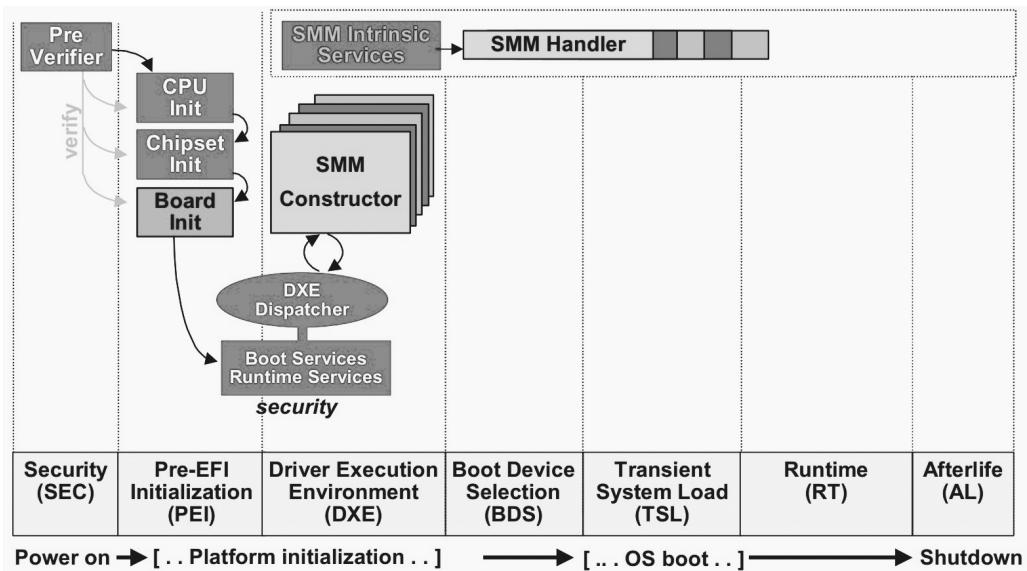


FIGURE 22: SMM Framework Architecture

4.2 System Management System Table (SMST)

System Management System Table (SMST) is core mechanism of SMM handler to pass information and enabling activity.

SMST table allows access to service based on the SMST which also known as SMM Services. Driver can only use SMM services during execution inside context of the SMM. `EFI_SMM_BASE_PROTOCOL.GetSmstLocation()` service used to discover the address of SMST.

SMST is a set of potentiality exported for utilization by any driver that is loaded into SMRAM. It's similar to the EFI System Table except that by design it's fixed set of services and data and also doesn't acknowledge to the resiliency of an EFI protocol interface.

SMM infrastructure component of Framework provides SMST, which manages:

- Dispatching drivers inside SMM
- Allocation of memory (SMRAM)
- Switching the framework in and out of the applicable SMM of the processor

4.3 SMM and Available Services

4.3.1 SMM Services

As EFI runtime drivers have their constraints, similarly the model of SMM framework will have them too. Especially, dispatch of drivers in SMM won't be capable of using any core protocol service. However SMST-based services, called SMM Services allows the drivers to be access using an SMM identical of the EFI System Table, but services of the core protocol won't grantee the availability in runtime. As an alternative, the complete mass of EFI Boot Services and EFI Runtime Services can be available while the driver loading or "constructor" phase.

With utilizing the visibility of constructor, SMM driver is capable to leveraging rich set of EFI service to perform:

- Marshall interface for EFI services.
- Observing EFI protocols which are populated by other SMM drivers while in constructor phase.

For drivers while not in SMM and during the initial load inside SMM, EFI protocol database becomes quite useful by utilizing design.

Available services which are SMST-based includes:

- Negligible, blocking kind of the device Input/Output protocol
- Memory allocator from SMRAM

These services are exposed through the entries present in the System Management System Table (SMST).

4.3.2 SMM Library

During constructor phase of SMM driver inside SMM, all additional service within SMM Library (SMLib) are uncovered like EFI protocols. i.e., An identical status code in SMM is merely an EFI protocol with interface referencing an SMM-based driver service. To avoid error or information of progress during runtime, other SMM drivers also locates this SMM based status code.

4.4 SMM Drivers

4.4.1 Process to Load Drivers in SMM

Process to load driver modal in SMM is merely a DXE SMM runtime driver having a DEPEX (dependency expression) having at least `EFI_SMM_BASE_PROTOCOL`. This kind of dependency is essential as the DXE runtime driver which is planned for SMM will utilize the `EFI_SMM_BASE_PROTOCOL` to load up itself again in SMM and re-execute its entry point. Also, other SMM-loaded protocols permitted to be stayed in the DEPEX of specified SMM DXE runtime driver. Principle of the DXE Dispatcher is to verifying if the GUIDs to be consumed by the protocols does exists in the database of protocol and capable to identifying if the driver can be loaded or not.

After formerly loaded in SMM the DXE SMM runtime driver becomes capable utilize only minor set of services. While in its constructor entry point, the driver can use EFI Boot Services as it executes within space of boot service and SMM.

In secondary entry point in SMM driver is capable to perform:

- Registration of an interface - In the formal protocol database, naming the SMM occupant interfaces with future-loaded SMM drivers
- Registration with the SMM codebase - For a callback hook in effect to an SMI pin stimulation or an SMI based interrupt message from outside of SMM Code (i.e. a boot service, runtime agent)

After this **constructor** phase in SMM, the SMM driver needs not be rely on any other boot services as the mode of operation to carrying out execution can move away from these services. Many EFI Runtime Services could possess the majority of their execution shifted into SMM and viewable runtime portion simply becomes a proxy which merely utilizes the `EFI_SMM_BASE_PROTOCOL` to perform callback in SMM to carry out services. By Possessing a proxy which allows for a modal of sharing code blocks of error handling, like services for flash access and also the EFI Runtime Services `GetVariable()` or `SetVariable()`.

4.4.2 SMM Drivers for IA-32

In SMM the “IA-32 runtime drivers” can not called as on the image the action by `SetVirtualAddress()` is performed. Hence, code segment that requires to be accessible among SMM and EFI runtime needs to be migrated in SMM.

4.4.3 "Itanium® Processor Family" SMM Drivers

From “Platform Management Interrupt (PMI)” the runtime drivers for the “Itanium® processor family” are called as if each of them is kind of “Position Independent Code (PIC) runtime driver”.

4.5 SMM Protocols

System Architecture of SMM broke in to below two parts:

- “SMM Base Protocol” - exposed by the processor. This protocol is liable to perform:
 - To initialize the state of processor
 - Registration of the handlers
- “SMM Access Protocol” - interprets the specific enabling and locking mechanism that an IA-32 memory controller may allows during execution in SMM. (Not needed for “Itanium® processor family”)

4.5.1 SMM Protocols for IA-32

Figure 23 shows the SMM protocols which are published for an IA-32 system.

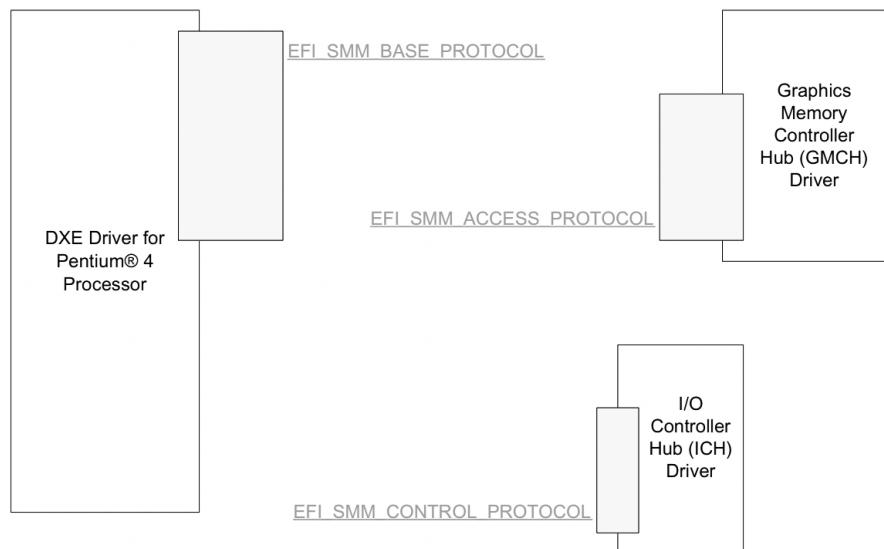


FIGURE 23: Protocols Published for IA-32 Systems

4.5.2 SMM Protocols for "Itanium®-Based Systems"

Figure 24 shows the way SMM protocols are published for an “Itanium®-Based system”.

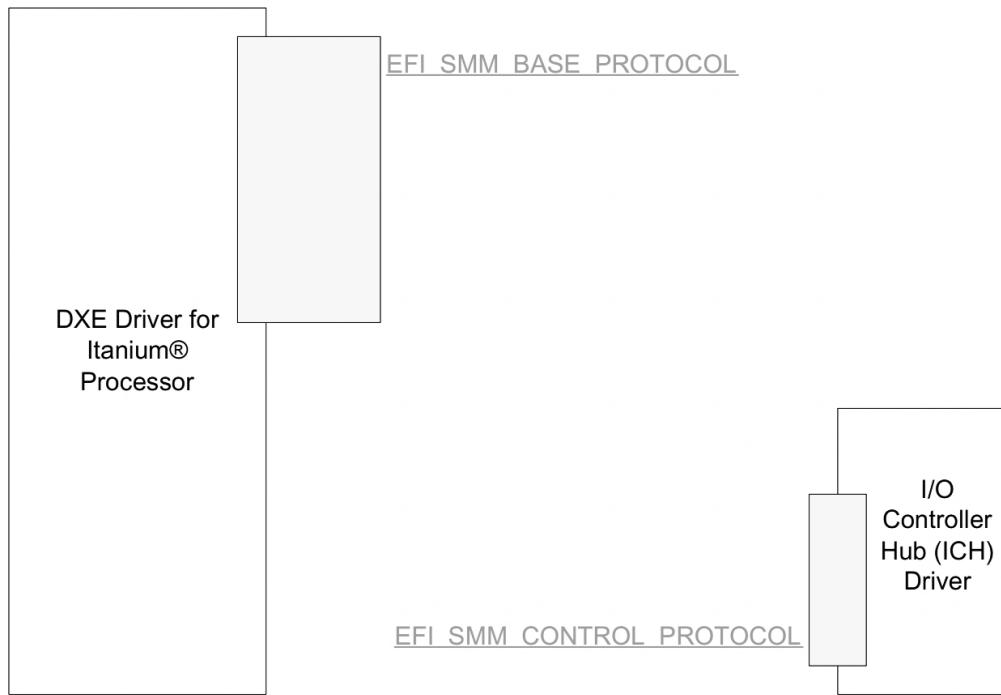


FIGURE 24: Protocols Published for "Itanium®-Based Systems"

4.6 SMM Dispatcher and infrastructure

SMM Code segment lies within the SMM Dispatcher. Major Role of SMM Dispatcher is to give the control mode to the SMM handlers in a systematic methodology. SMM Infrastructure Code aids to drive communication for SMM to SMM. SMM handlers are PE32+ images.

4.7 Initializing SMM Phase

The SMM driver for the Framework is fundamentally a enrollment transport mode to dispatch the drivers in outcome to the:

- System Management Interrupts for IA-32
- Platform Management Interrupts (PMIs) for Itanium® processor family

4.8 Relation of "System Management RAM (SMRAM)" to conventional memory

Figure 25 shows relationship between SMRAM and main memory in IA-32. Where SMRAM is isolated secure part inside the conventional main memory.

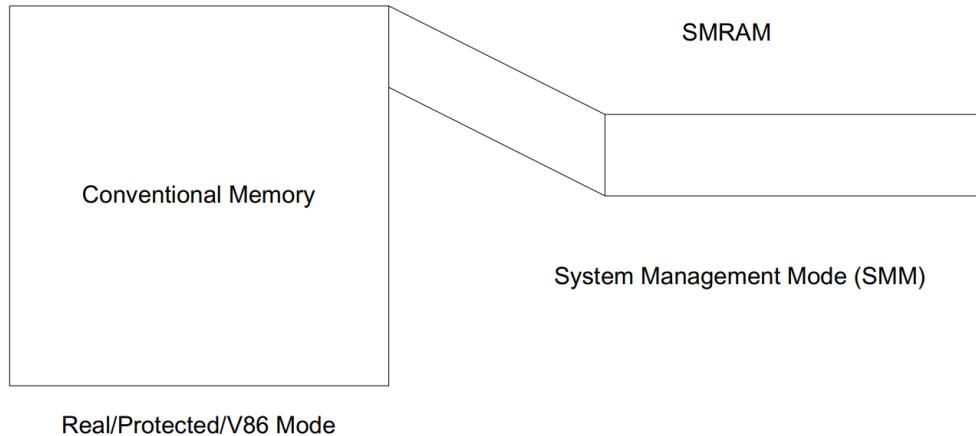


FIGURE 25: SMRAM kinship with conventional memory

4.9 Execution Mode of SMM on Processor

SMM is accessed asynchronously with the ongoing main flow of program. SMM was primitively developed to be clear to the OS and provide a power management facility more transparent.

Preboot agents are responsible to initiate alternate uses of SMM which are:

- Applicable Workaround for SoC exaggeration
- Logging of error(s)
- Security for the platform

A SMI can be launched by energizing either the SMI logic pin via dedicated on the board or by utilizing the local APIC.

“Itanium® architecture” possess no independent separate mode for processor for the tractability of interruption however it does supports “Platform Management Interrupt (PMI)” which indeed is a maskable interruption. However, there is this another way to enter PMI using a interrupt message on local “Streamlined Advanced Programmable Interrupt Controller (SAPIC)”.

This architecture informs a techniques to load modules of needful code segment that substantiate the functionality specified above. The internal representation of protocol which enables the loading of images of various handler and runs in normal memory of boot-services. Only the handlers does to run in SMRAM.

4.10 Accessing Platform Resources

As per policy outcome process of the execution of SMM handlers is reasonably prevents from accessing conventional memory resources. Hence, there does not exist any ease binding technique such as a call or trap interface to render the services in preemptive bid of non-SMM state.

Besides, SMM Services - the library of service which abides a sub set of the core EFI services, i.e. device input-output protocol, memory allocation and others. Also, execution mode of SMM driver has the equivalent structure as per the EFI criterion - namely a components which executes under boot services and it could perhaps run in runtime mode. When `ExitBootServices()` invoked, the mechanism of an unregister event occurs.

5. Proposed Work

In general to generate BIOS image (*.rom file), compilation of XYZ.c (source code) has to be done, this compilation not only involves compilation of DXE driver, PEI driver, EFI Application but also includes pre-processing checks, compression of raw files which takes huge amount of time depending on the system configuration. Implementation of this project aids in reduction of this compilation time.

5.1 Stake holders

The proposed work is applicable but not limited to below stake holders:

- **BIOS development team** : main development group in contributing BIOS firmware, this is the only stake holder who are having access to the BIOS development environment and access to the source code of the complete BIOS firmware
- **Validation team** : performs various validation on developed BIOS image
- **Automation team** : brings various integration and validation automation to module(s)
- Other Development team who wishes to ease the debugging process

5.2 Issues

The Proposed work is capable of mitigating below issues:

- Generation of BIOS image - includes compilation of whole source code
- Time complexity - took enormous amount of time to generate the BIOS image
- Accessing and modifying BIOS Setup Option(s) remotely
- Firmware Flashing of BIOS remotely
- Updating CPU microcode
- Summarizing changes among BIOS image
- Avoiding exposing the source code support for OEM to fill their OEM information
- Avoid setting of BIOS development platform for stake holders which are not meant to be the BIOS developer
- Runtime BIOS Support for temporary UEFI variable creation

5.3 Requirements

5.3.1 Software Requirements

- Visual C/C++ binaries
- Python 3
- Visual Studio Code (IDE)
- Memory Access Interface - supported mechanism to communicate over target memory

5.4 Development Process of Modules

Framework development process is driven by implementation of independent modules which can serve functionality and having flexibility to integration to the framework.

5.5 Module: Setup Knob modification

5.5.1 Processing Unsigned debug BIOS

Before Releasing the BIOS firmware for public use, those are signed for security and integrity purpose, however the debug BIOS which are used Pre-release to test and verify all the functional features until all the requirements are met.

Every SoC system which are under test known is SUT are configured in such a way that it supports debug BIOS. The proposed framework is designed to simulate the process of SUT in terms of processing BIOS binary similar to SUT performs it after flashing BIOS firmware on SoC.

Processing the debug BIOS can be classified in to two ways:

1. Applying changes directly to the SUT
2. Applying changes on to the BIOS image

At the high level the flow for both the above classification remains the same but will be differentiated at the backend support. An additional driver is attached with BIOS firmware to aid the framework to be able to apply changes directly to the SUT.

5.5.2 Additional Tech Stack Used

Below are the listed technologies consumed in development of this module in addition to the already specified requirements in Section 5.3

- Tkinter
- XML
- JSON

5.5.3 Flow of the module

Figure 26 describes the flow of setup knobs modification on the System Under Test (SUT).

The iteration of the development could be reduce in two ways:

1. Processing Debug/Unsigned BIOS in section 5.5.1
2. Processing Firmware individually in section ??

5.5.4 Screenshots of Module

As a PoC for the framework, this section shows snapshots of the working module to mimic the setup options of BIOS, however as a simulation framework, it also provides quite more features which are not available in the actual BIOS due to memory limitation.

Figure 27 shows the prompt asked to user to select basic configurations before launching the module of framework. Configurations available to select are:

- Working Mode (options to be selected as in figure 28)
 - online - to work on SUT and require to select valid access method for online mode from menu
 - offline - to work on BIOS binary
- Access Method - selecting valid access method for working on SUT
- Publish all? - Boolean options to decide whether to evaluate DEPEX or not.

Table 9 describes the interpretation of each button action on specific condition as remarks if applicable

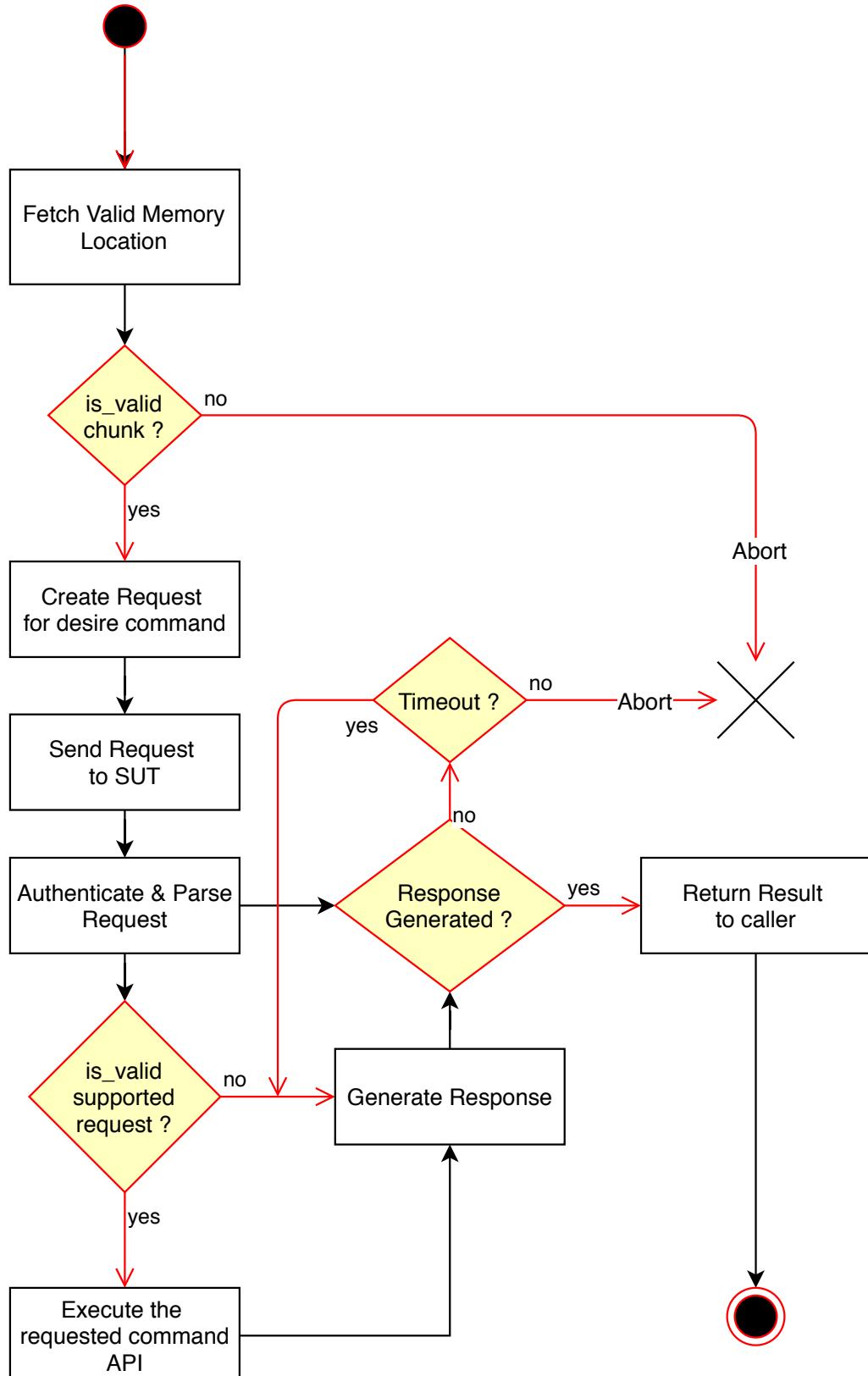


FIGURE 26: Flow of Setup Knobs Modification

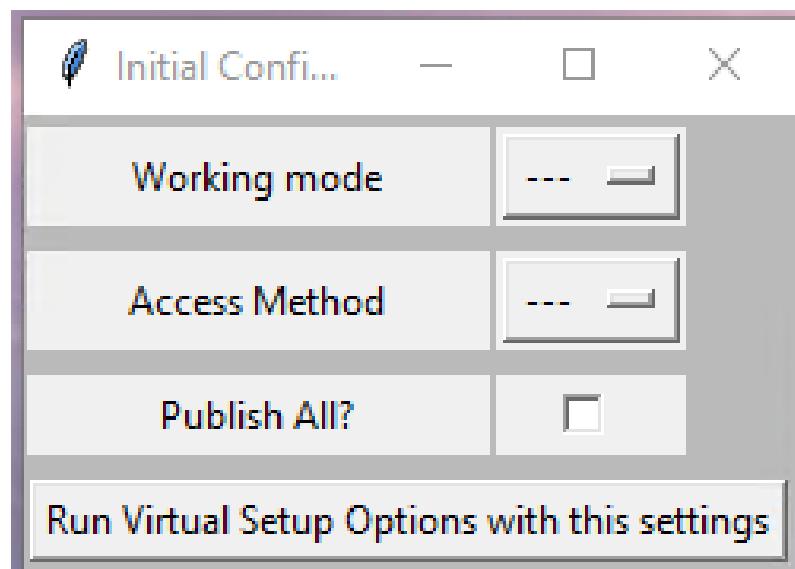


FIGURE 27: Menu to Select initial configuration for work

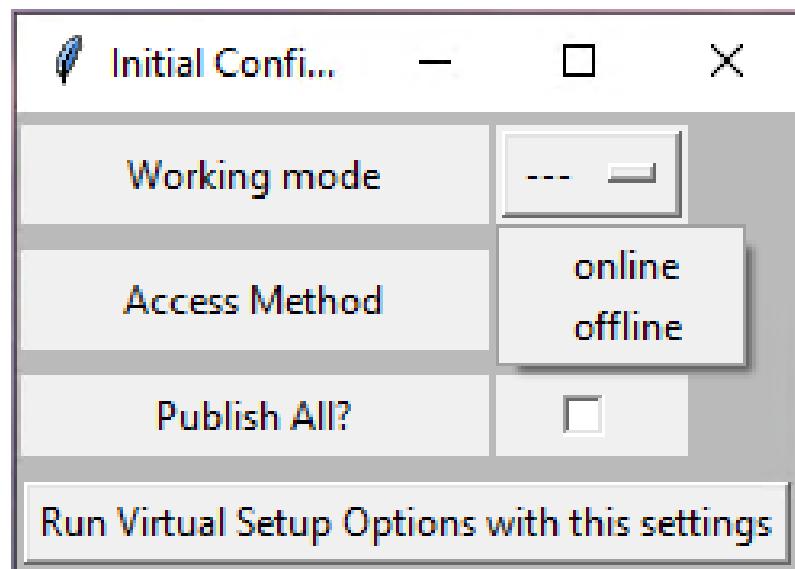


FIGURE 28: Available work mode for the system: Online and Offline

5.5.5 Outcome of Module

- The module is capable of cross platform usage.
- The module can work with all the platform binary and SUT.
- A communication bridge as a driver in BIOS firmware to aid the framework run directly on SUT is implemented.
- Generic solution is provided for end-user while running any of the classification listed in 5.5.1.

TABLE 9: Interpretation of buttons on Virtual Setup Page GUI

Button	Interpretation
Push Changes	Apply changes to system if online mode else apply changes to 'bin' file
View Changes	View saved changes in new window
Exit	Exit the GUI
Reload	Reload the GUI
Discard Changes	Discard any change made, any value if modified are restored to current value
Load Defaults	Restore to default values and revert any changes made

- Simulating the information from system or binary image is provided as native GUI application.
- Real time sync with simulation framework is supported.
- Seamless Integration of any new features or modules in framework is made possible.

5.6 Module: Parsing

Figure 29 represents the overview of the BIOS as a File system which is interpreted and parsed from the BIOS image. Detail architecture of the same is explained in Section 3.

5.6.1 Additional Tech Stack Used

Below are the listed technologies consumed in development of this module in addition to the already specified requirements in Section 5.3

- Decompression binaries
- XML
- JSON

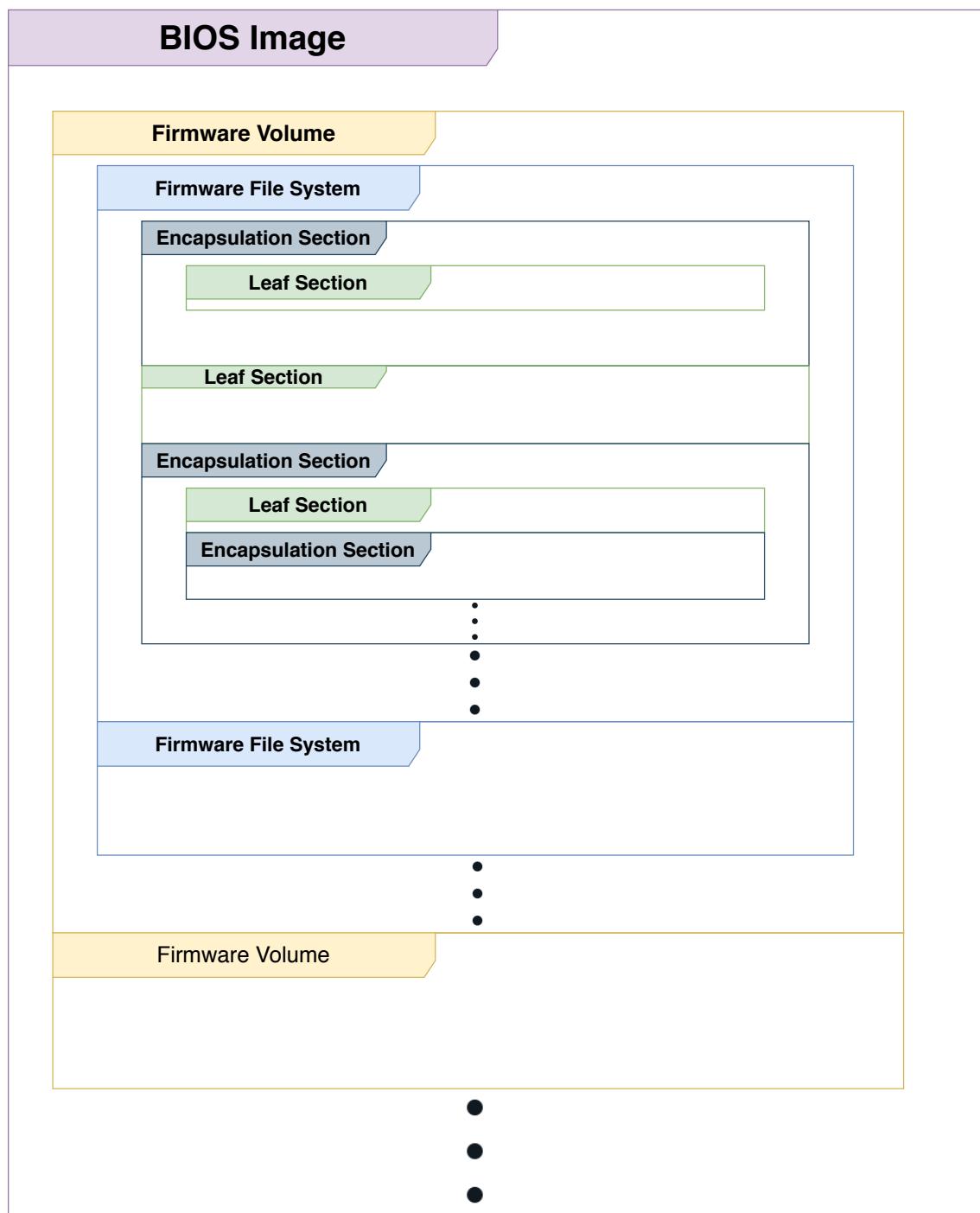


FIGURE 29: Overview of BIOS image as a File System

5.6.2 Flow of the module

Figure 30 describes the flow of the Parsing module. The Initial part is performed by user who is responsible to select valid memory interface to work. Note that some memory interface are supported by the module which requires additional hardware and software setup which are considered to be the part of dependency of interface itself which is not in the scope of the module.

When User select valid Interface the module will determine whether user is on Target SUT or on the local BIOS image. If user is working on SUT with valid memory interface and privileges then BIOS image will be parsed from the memory.

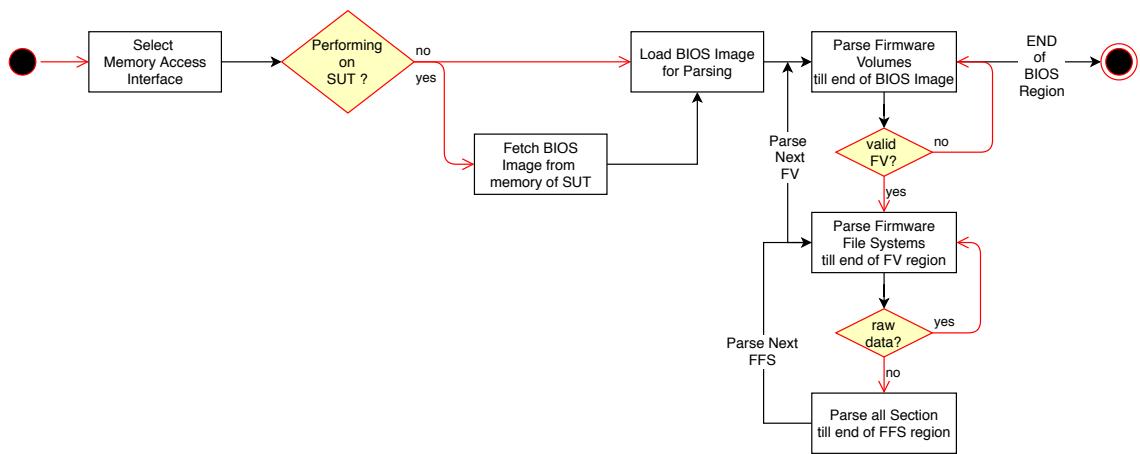


FIGURE 30: Flow of Parser

As on both the cases BIOS Image is available to act on, the module will start the parsing of the BIOS image as interpretation described in Figure 29. It parses All the valid firmware volumes only till the end of BIOS image (skips the free space or firmware volumes with invalid signature and GUID). Decompression of file system under the firmware volume if any is handled by the module too, for the decompression of file system it uses the binary for decompression technique available to public i.e. lzma, tianocore, brotli etc.

5.6.3 Outcome of Module

- Human Readable interpretation of BIOS image is provided.
- Possible to debug the BIOS via setup knobs comparison.
- Lookup of order of the module in BIOS image as readable file system is also possible.
- Verification of integration of module via GUID can be done.
- Extracting and storing file system or module of BIOS image by GUID
- Summarizing changes of two BIOS image

5.7 Module: Runtime UEFI variable Creation

Each variable in BIOS has a scope for each variable where Runtime support is one of the attribute, to simply state the run time variable one can interpret it as the variable which will be available during and after the completion boot flow (while OS is running). Such a variable require special access mechanism, which is carried out by the System Management mode SMM described in Section 4..

Earlier Challenges are described as below:

- Providing and maintaining native driver support from BIOS for creation of UEFI variable
- Setting of Build environment for non-BIOS development team

Note: As all the variable created at runtime the scope of such variable are limited to the flashing of the BIOS. i.e. when BIOS is flashed/re-flashed or updated, those variable won't be available on the SUT.

5.7.1 Additional Tech Stack Used

Below are the listed technologies consumed in development of this module in addition to the already specified requirements in Section 5.3

- Flask
- Ajax
- jQuery
- Javascript
- HTML/CSS
- XML
- JSON

5.7.2 Flow of the module

The Flow of the module is described in section 5.7.3 along with screenshots which is easier to interpret the flow chart in Figure 31.

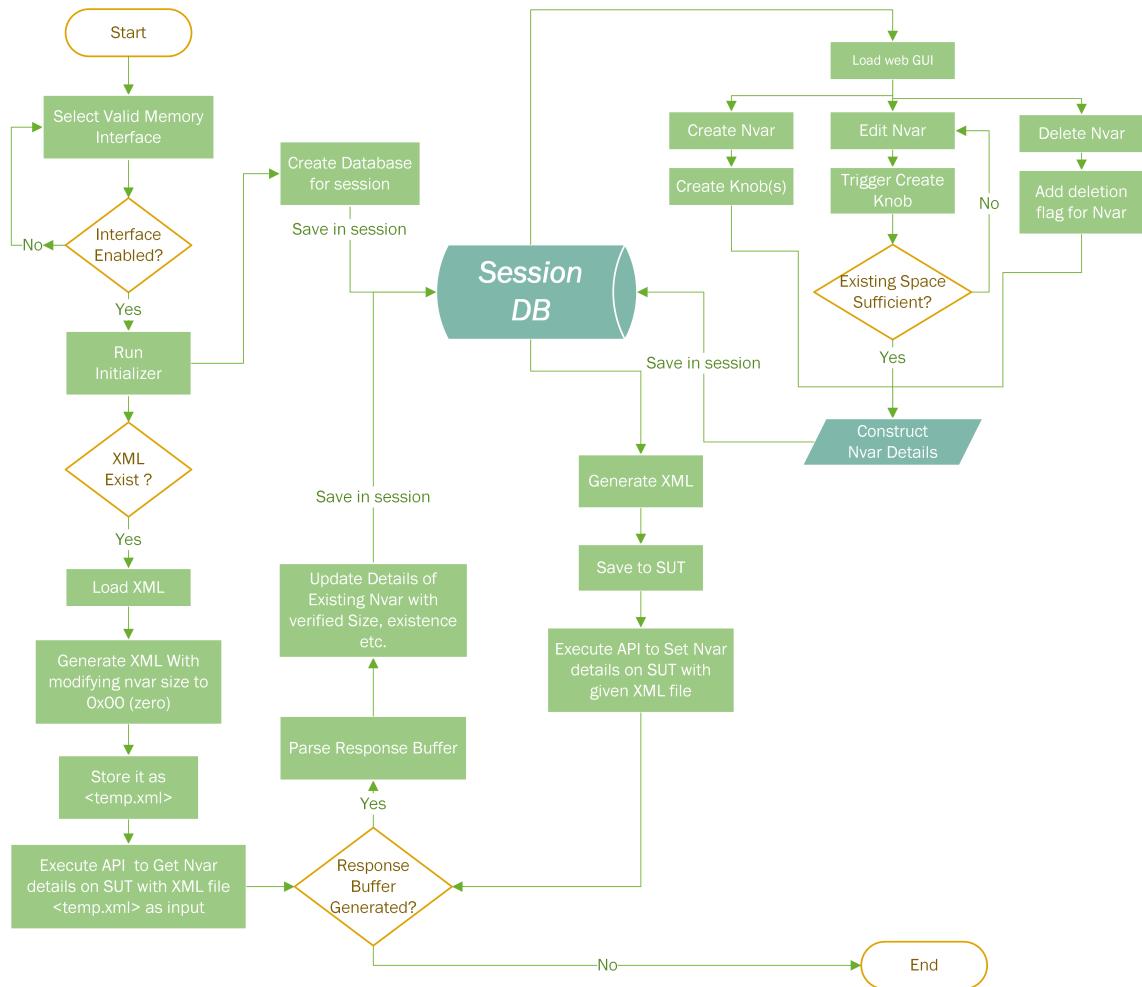


FIGURE 31: Flow of Nvar Web GUI

5.7.3 Screenshots of Module

Whenever the User launches the module the home page screen to select valid communication interface will appear as displayed in Figure 32. This is the crucial stage as if valid interface for communication is not selected one may not be able to use the functionality of the service.

After selection of valid Interface one may operate the desired options listed in navigation bar which are:

Figure 33 lists the variable created under the current session which is to be applied

Figure 34 displays form which allows user to create Variable, where user needs to specify the name of the variable with certain restriction of input field. To identify and lookup the Variable the GUID is required which is automatically generated by the module with required format, however if user wishes then they can modify the GUID.

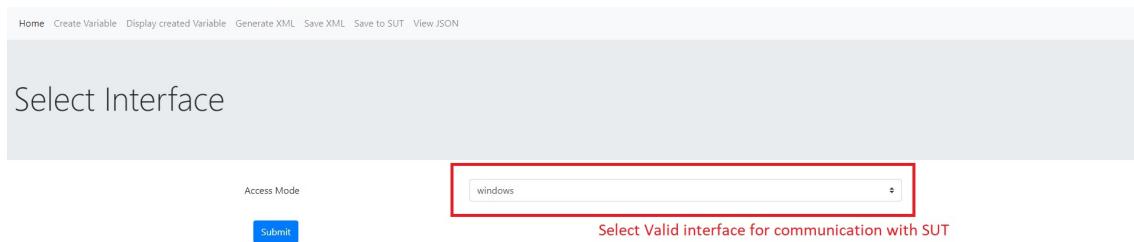


FIGURE 32: Home Page to Create UEFI Variable

TABLE 10: Navigation Bar Action

Button	Interpretation
Create Variable	Opens a form to create new Variable as in Figure 34
Display Created Variable	lists out created variable as in Figure 33
Generate XML	Generate XML from the stored session database as in Figure 41
Save XML	Saves the generated XML on the storage device
Save to SUT	Applies the Pending changes action (Create/Delete/Modify) to the SUT
View JSON	View the stored session database in the json format as in Figure 42

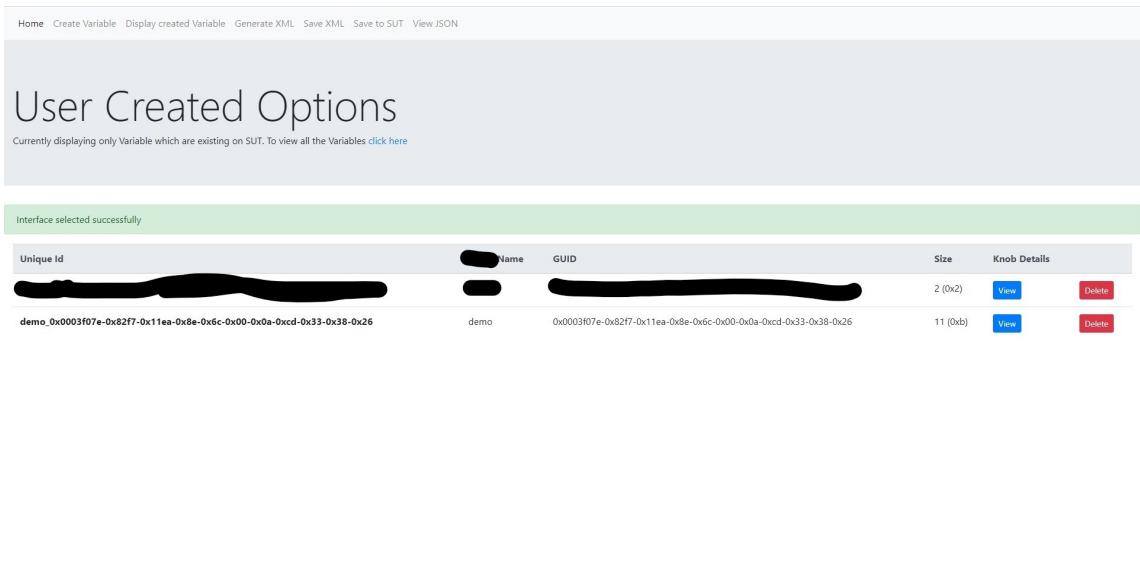


FIGURE 33: Variables created or exists on SUT

Variable name	<input type="text" value="Enter Variable Name (only alphabets and numbers allowed)"/>
GUID	<input type="text" value="0xbff24c08-0x873c-0x11ea-0x98-0xde-0x00-0x0a-0xcd-0x33-0x38-0x26"/>
Attributes	<input type="text" value="0x7"/>
<input type="button" value="Submit"/>	

FIGURE 34: Create new UEFI Variable on SUT

Figure 35 opens the list of the options if created and allows to edit their current values too. However one can also add the new option to the Variable. It allows user to create various types of options under the variable which are oneof type as in Figure 37, string type as in Figure 38, numeric type as in Figure 39 and the checkbox type which allows user to toggle the option value in as Boolean interpretation. Common fields for creating options including its name, type, description and size.

If user wants to change the value set for the variable created while creation of option as described in Figure 36 forms one can actually modify the value.

The highlighted prompt in Figure 37 allows user to create the choices for the option where one of the multiple values to be selected as a result, By clicking Add Option

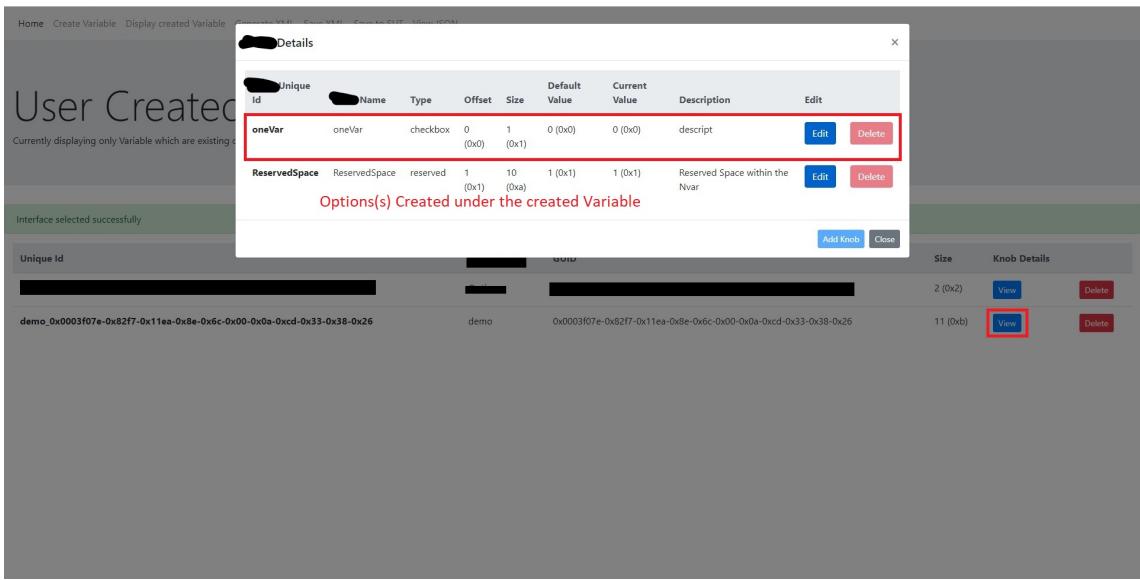


FIGURE 35: Options listed under Variable

Variable name	demo	Type	Offset	Size	Default Value	Current Value	Description	Edit
Guid	0x0003f07e-0xd2f7-0x11ea-0x8e-0x6c-0x00-0x0a-0xcd-0x33-0x38-0x26	oneVar	oneVar	checkbox	0 (0x0)	1 (0x1)	0 (0x0)	descript
Size	11 (0x6)	ReservedSpace	ReservedSpace	reserved	1 (0x1)	10 (0xa)	1 (0x1)	Reserved Space within the Nvar
Is_exist	True (0x1)							
Attributes	7 (0x7)							
Name	oneVar							
Type	checkbox							
Value	0 (0x0)							
Current_value	0 (0x0)							
Size	1 (0x1)							
Offset	0 (0x0)							
Description	descript							

FIGURE 36: Edit the Existing Option Created under Variable SUT

button user can create choices and under drop down menu besides Value, user can select default value to be selected for the option.

Option type string as in Figure 38 allows user to create a option which accepts minimum and maximum characters to be supported in the string as well as the default string value to be selected.

To set the numeric input for the option, minimum and maximum value along with the default value to be set as in Figure 39

For the future use one can create a reserved space under the UEFI variable as in Figure 40

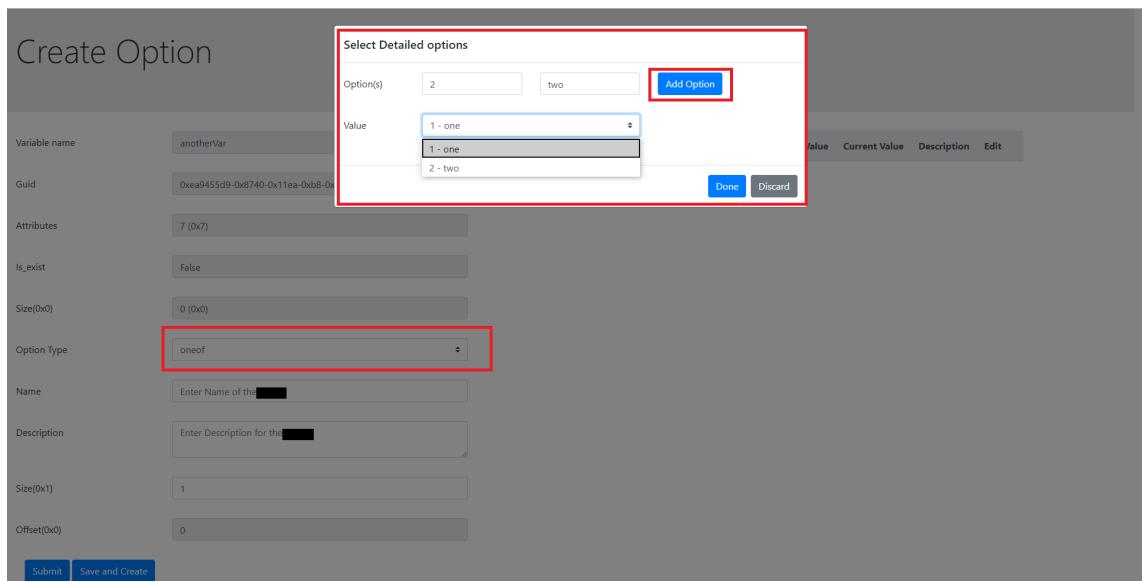


FIGURE 37: Create New Option(s) under Variable - Oneof Type

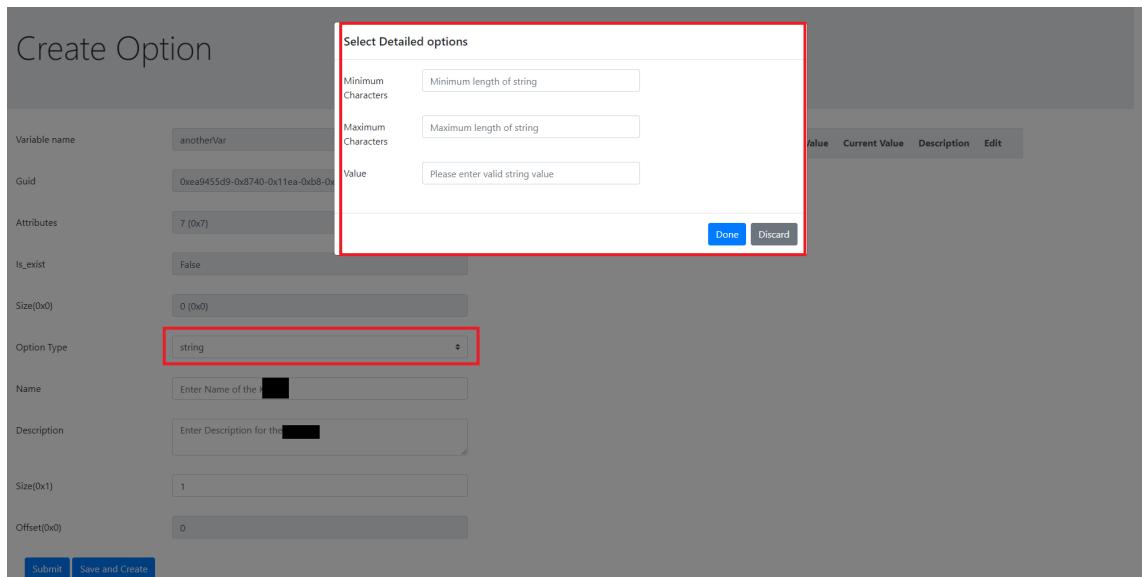


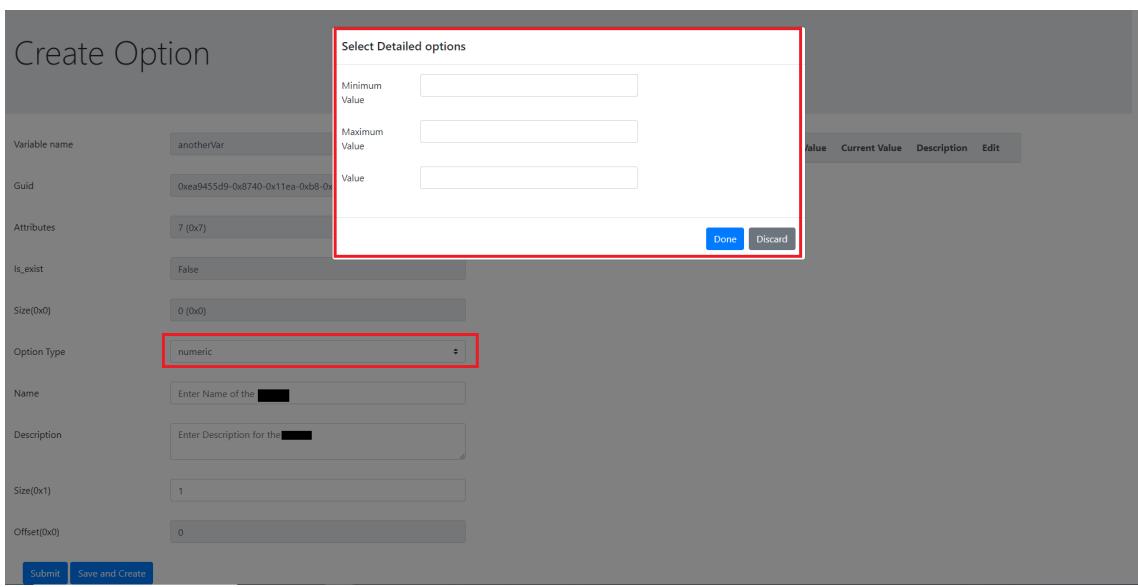
FIGURE 38: Create New Option(s) under Variable - String Type

Figure 41 shows the XML which is generated from the existing and newly created variables and options under it.

Figure 42 represents session data of existing and newly created data (if any) as json

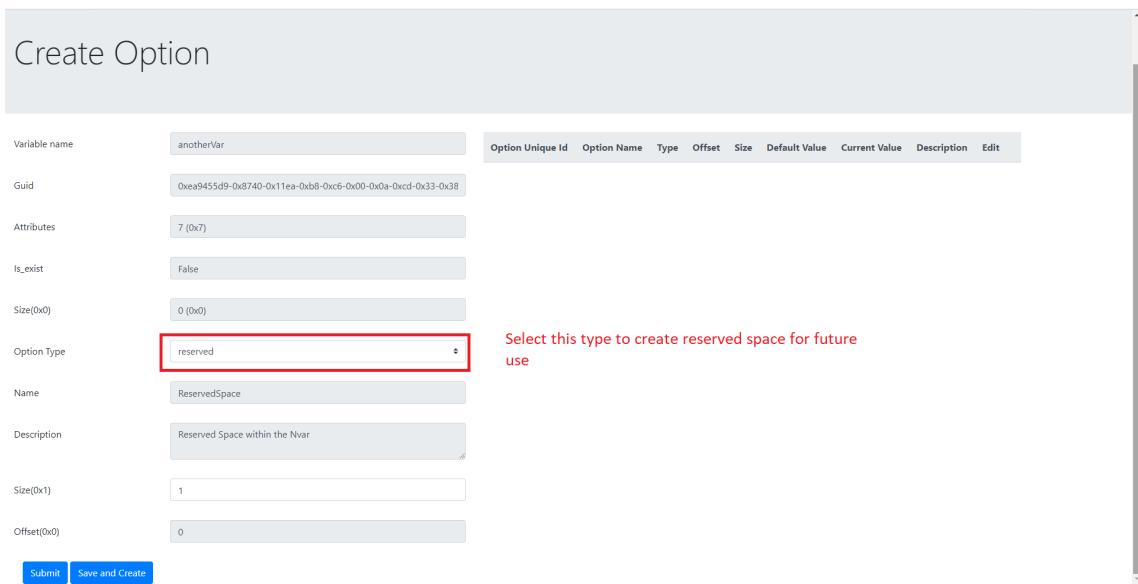
5.7.4 Outcome of the module

- Enables creation of UEFI variable from OS layer.



The screenshot shows the 'Create Option' dialog box. At the top, it says 'Create Option'. Below that, there are several input fields: 'Variable name' (anotherVar), 'Guid' (0xea9455d9-0x8740-0x11ea-0xb8-0xc6-0x00-0x0a-0xcd-0x33-0x38), 'Attributes' (7 (0x7)), 'Is_exist' (False), 'Size(0x0)' (0 (0x0)), 'Option Type' (numeric, highlighted with a red box), 'Name' (Enter Name of the [redacted]), 'Description' (Enter Description for the [redacted]), 'Size(0x1)' (1), and 'Offset(0x0)' (0). At the bottom are 'Submit' and 'Save and Create' buttons. A modal window titled 'Select Detailed options' is open, showing 'Minimum Value' (empty), 'Maximum Value' (empty), and 'Value' (empty). There are 'Done' and 'Discard' buttons at the bottom of the modal. The entire 'Select Detailed options' window is also highlighted with a red box.

FIGURE 39: Create New Option(s) under Variable - Numeric Type



The screenshot shows the 'Create Option' dialog box. The fields are the same as in Figure 39: 'Variable name' (anotherVar), 'Guid' (0xea9455d9-0x8740-0x11ea-0xb8-0xc6-0x00-0x0a-0xcd-0x33-0x38), 'Attributes' (7 (0x7)), 'Is_exist' (False), 'Size(0x0)' (0 (0x0)), 'Option Type' (reserved, highlighted with a red box), 'Name' (ReservedSpace), 'Description' (Reserved Space within the Nvar), 'Size(0x1)' (1), and 'Offset(0x0)' (0). A tooltip 'Select this type to create reserved space for future use' appears next to the 'reserved' option type. At the bottom are 'Submit' and 'Save and Create' buttons.

FIGURE 40: Create Reserved Space for future use under Variable

- Lifts headache of maintaining variable creation from BIOS development for individuals.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```

<!-- Generated by [REDACTED] -->
<Nvar name="Option" Guid="0xbff24c08-0x873c-0x11ea-0x98-0xde-0x00-0x0a-0xcd-0x33-0x38-0x26" Attributes="0x7" Size="0x2">
  <knob name="revision" setupType="numeric" default="0x1" CurrentVal="0x7" size="0x1" offset="0x0" description="Revision number" min="0x0" max="0xff"/>
  <knob name="SubOption" setupType="oneof" default="0x4" CurrentVal="0x4" size="0x1" offset="0x1" description="option descriptions..."/>
    <options>
      <option text="option 1" value="0x0"/>
      <option text="option 2" value="0x1"/>
      <option text="option 3" value="0x2"/>
      <option text="option 4" value="0x3"/>
      <option text="option 5" value="0x4"/>
    </options>
  </knob>
</Nvar>
<Nvar name="demo" Guid="0x0003f07e-0x82f7-0x11ea-0x8e-0x6c-0x00-0x0a-0xcd-0x33-0x38-0x06" Attributes="0x7" Size="0xb">
  <knob name="oneVar" setupType="checkbox" default="0x0" CurrentVal="0x0" size="0x1" offset="0x0" description="descript"/>
  <knob name="ReservedSpace" setupType="reserved" default="0x1" CurrentVal="0x1" size="0xa" offset="0x1" description="Reserved Space within the Nvar"/>
</Nvar>
</SYSTEM>

```

FIGURE 41: Generate XML SUT

```

{
  "Option_0xbff24c08-0x873c-0x11ea-0x98-0xde-0x00-0x0a-0xcd-0x33-0x38-0x26": {
    "attributes": "0x7",
    "guid": "0xbff24c08-0x873c-0x11ea-0x98-0xde-0x00-0x0a-0xcd-0x33-0x38-0x26",
    "is_exist": false,
    "knobs": {
      "SubOption": {
        "current_value": "0x4",
        "description": "option descriptions...",
        "knob_type": "oneof",
        "name": "SubOption",
        "offset": 1,
        "options": [
          {
            "text": "option 1",
            "value": "0x0"
          },
          {
            "text": "option 2",
            "value": "0x1"
          },
          {
            "text": "option 3",
            "value": "0x2"
          },
          {
            "text": "option 4",
            "value": "0x3"
          },
          {
            "text": "option 5",
            "value": "0x4"
          }
        ],
        "size": 1,
        "value": "0x4"
      },
      "revision": {
        "current_value": "0x7",
        "description": "Revision number",
        "knob_type": "numeric",
        "max_value": "0xff",
        "min_value": "0x0",
        "name": "revision",
        "offset": 0,
        "size": 1,
        "value": "0x1"
      }
    },
    "next_offset": "0x2",
    "nvar_name": "Option",
    "old_size": 0,
    "size": 0,
    "size_mismatch": true
  },
  "demo_0x0003f07e-0x82f7-0x11ea-0x8e-0x6c-0x00-0x0a-0xcd-0x33-0x38-0x26": {
    "attributes": "0x7",
    "guid": "0x0003f07e-0x82f7-0x11ea-0x8e-0x6c-0x00-0x0a-0xcd-0x33-0x38-0x26",
    "is_exist": true,
    "knobs": {
      "ReservedSpace": {
        "current_value": "0x1",
        "description": "Reserved Space within the Nvar",
        "knob_type": "reserved"
      }
    }
  }
}

```

FIGURE 42: Generate XML SUT

6. Future Scope of Work

Few implementation modules of Section 5. are not well developed at production launch which a slight modification and standard checks have to be performed to make the modules qualify for production level. Also as the release of production other stuff to be maintained is user guide, FAQs and other "how-to" articles to help out others to ease in using the framework.

Along with the enhancing of existing modules there will still be exercise to analyze existing system to explore more use cases which are taking a longer time for every build iteration for the system.

Few of the possible use cases to study and decide the feasibility of implementation would be:

- Development and testing of individual driver component rather than building the whole BIOS image
- AI powered Search Engine to enhance the findings of FAQs for relevant existing queries and articles
- Automating the initial BIOS Environment Setup
- Platform independent easy installation setup for the framework

Glossary

ACPI Advanced Configuration and Power Interface . iii, v, viii, 1, 5, 6

BDS Boot Device Selection . vi, 20, 25

BIOS Basic Input Output System . iii, v, 1, 2, 5

CSME Converged Security and Mobility Engine . 61

DEPEX Dependency Expression . 25, 54

DXE Driver Execution Environment . vi, 20, 25, 30

EDK II Extensible Firmware Interface Developer Kit II . 18, 21

FFS Firmware File System . vi, 30, 31, 39

FV Firmware Volume . vi, 25, 30, 31

GOP Graphics Output Protocol . v, 11, 14, 15

IFWI Integrated Firmware Image . 27, 28

IP Intellectual Property . iii, 52

OS Operating System . 1, 2

PCI Peripheral Component Interconnect . iii, 1

PCIe Peripheral Component Interconnect Express . v, 1, 8, 12

PEI Pre-EFI Initialization . vi, 20, 22, 23, 27, 30

PI Platform Initialization . vi, viii, 18, 20, 21, 30

PMI Platform Management Interrupt . 47, 50

PoC Proof of Concept . 54, 61

SAPIC Streamlined Advanced Programmable Interrupt Controller . 50

SEC Security . vi, 20, 21

SHA Secure Hash Algorithm . 52

SMI System Management Interrupt . 45, 50

SMM System Management Mode . vi, 45, 59

SMRAM System Management Random Access Memory . 50

SMST System Management System Table . vi, 45

SoC System on a Chip . iii, 1, 53

SUT System Under Test . 53, 54, 58

UEFI Unified Extensible Firmware Interface . v, vi, 1–5, 16, 18