April 2021

FIRMWARE CONFIGURATION INTEGRITY IDENTIFY

HP INC

Firmware Configuration Integrity Identify

Problem/Objectives

- **Modern computers become more and more complex, because it has lots of controllers and processors, even sensors, integrated in a system. For example, a system may have USB PD (Power Delivery) controller, Thunderbolt controller, Camera, Card Reader, fingerprint Reader…etc. Each controller/processor/sensor may have its own firmware, usually, the firmware is updatable.**
- **Firmware Best Know Configuration (BKC) was provided by vendor. Computer already was verified and get better quality.**
- **Current system firmware (BIOS) has dependent with various peripheral device firmware. Different configuration, system will get unknow behavior.**
    - Example, Intel platform of BIOS has deep dependent with Management Engine firmware.
- **Verification team always take much time to get firmware BKC information and check firmware (BKC) status by manual.**
- **In here, we provide automatic solution to help verification team. They can reduce verification time and get better verification quality.**

Abstract

Concept

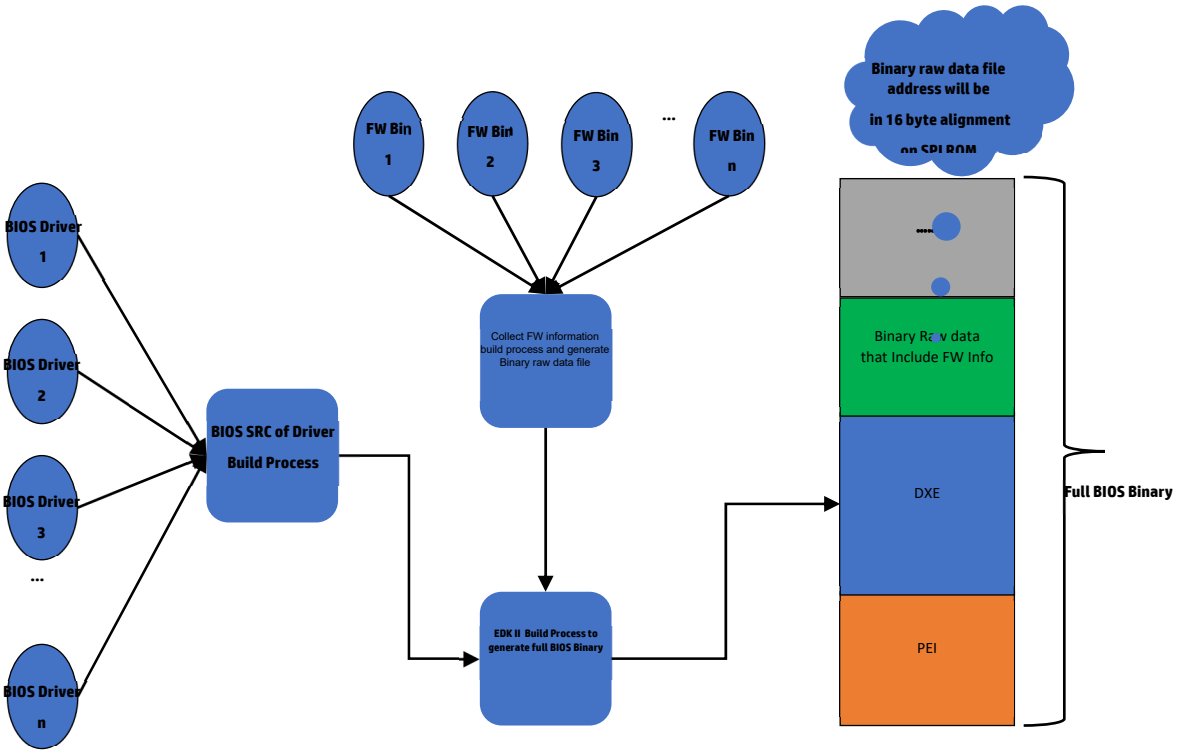
- *In system firmware (BIOS) develop phase, system firmware (BIOS) source code includes various peripheral devices firmware and configuration INF file.*
- *A binary raw data file that includes BIOS and various peripheral device firmware name, version, & vendor will be generate during BIOS build process.*
- *The binary raw data will be integrated into system firmware. Like, BIOS Logo file.*
- *A new SMBIOS type provides individual FW name, version, and vendor information.*
- *A warning message which firmware information doesn't match firmware BKC will display in pre-boot environment when system firmware is not protection.*

- *An error log that firmware doesn't match firmware BKC will always be record to support error management software tool.*
- *Two new WMI interface to return a binary raw data of various firmware information and error log. It can be utility on automatic verification software tool or error management software tool.*

Benefit

- ❑ Automatic firmware configuration integrity identifies in pre-boot environment.
- ❑ Reduce verification time resource and get better verification quality due to no human mistake parameter.
- ❑ New WMI interface provides expandable IT management capability.
- ❑ In protection BIOS, this innovation only will do error log without warning error message. No user experience impact.
- ❑ Help verification team to reduce resource and cost.

Product Drawing – BIOS Build Process



Product Drawing – (BKC)Binary RAW Data File Format

	Name			
GUID Definition (global GUID definition for WMI interface search BKC start pointer)				
Index 1 (1 byte length)	FW Name (ASCII String, terminated with a null "00h" byte)	FW Version	FW Vendor (ASCII String, terminated with a null "00h" byte)	00, 00 (terminated by a double-null "0000h")
….	…….	…….	…….	…….
Index N	FW Name	FW Version	FW Vendor	
Reserved. Binary raw data file size is 16 byte align. So Reserved file size is not fix. Reserved size = 16 – (total size % 16).				

FW version format definition:

- **Individual FW owns self firmware version definition. Example: Intel ME FW has 4 filed version definition. "11.22.33.44"**
- **In here, FW version utilities BCD format to describe full FW version information. Terminated with a null "00h" byte.**
- **Example. Intel ME FW information. 12.34.56.AE**

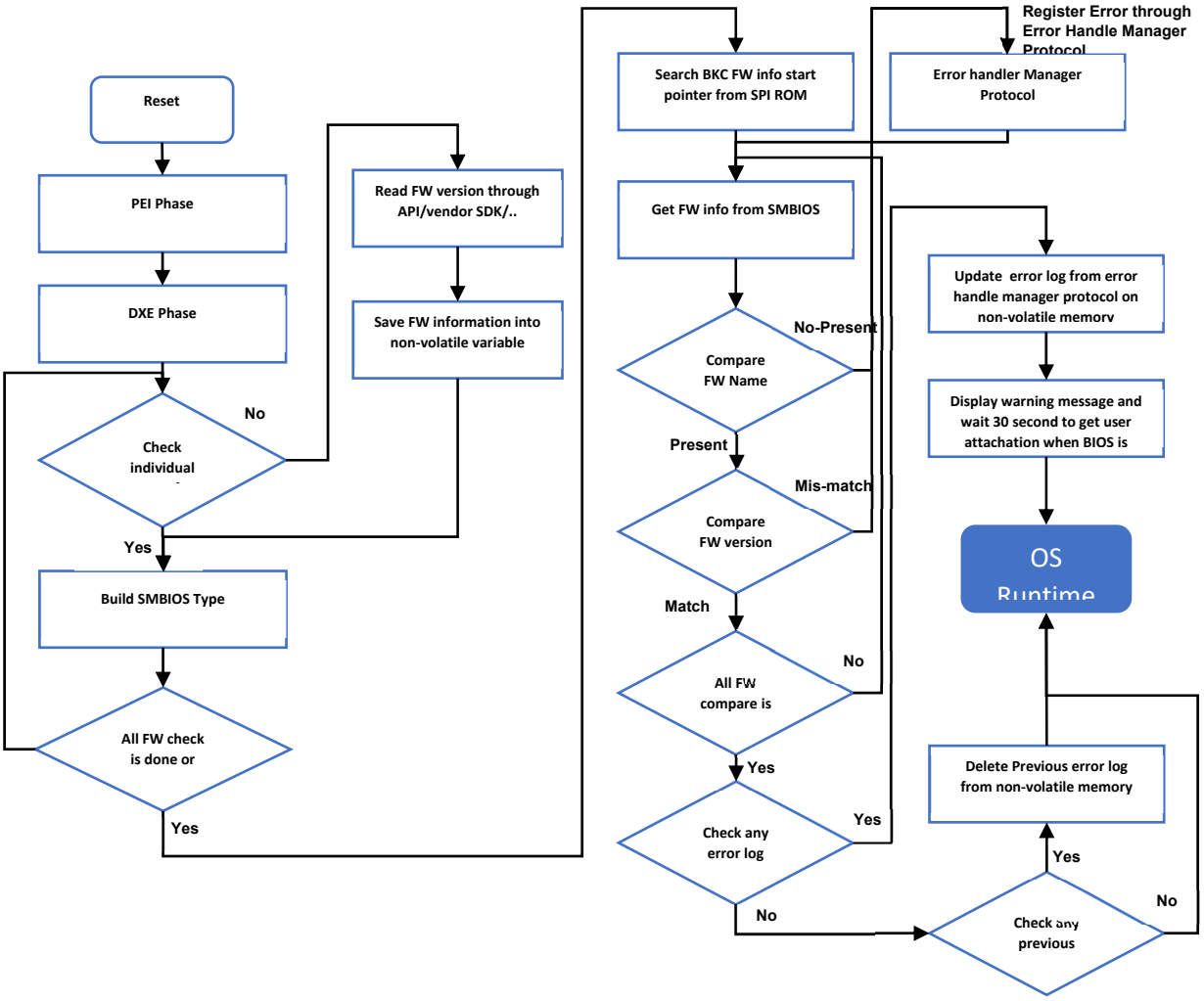
0x12	0x2E	0x34	0x2E	0x56	0x2E	0xAE	0x00

Product Drawing – SMBIOS Type definition

Offset	Name	Length	Value	Description
00h	Type	Byte	Varies	Specifies the type of structure. Types 128 through 256 (80h to FFh) are available for system- and OEM-specific information
01h	Length	Byte	05h	Specifies the length of the formatted area of the structure. String is not included.
02h	Handle	WORD	Varies	a unique 16-bit number in the range 0 to 0FFFEh
04h	FW Count	Byte	Varies	Total firmware count
05h	FW 1 Name	Byte	String	String number of the FW 1 Name (FW version format follow page 5)

06h	FW 1 Version	Byte	String	String number of the FW 1 Version (FW version format follow page 5)
07h	FW 1 Vendor	Byte	String	String number of the FW 1 Vendor (FW version format follow page 5)
……	……	…….	…….	……
05h + (n * 3)	FW n Name	Byte	String	String number of the FW n Name (FW version format follow page n)
06h + (n * 3)	FW n Version	Byte	String	String number of the FW n Name (FW version format follow page n)
07h + (n * 3)	FW n Vendor	Byte	String	String number of the FW n Name (FW version format follow page n)

Product Drawing –



Disclosed by Rick Hsia, Jimmy Kuo, Tom Hung, Harry Chang, Nicholas Feng, HP Inc.