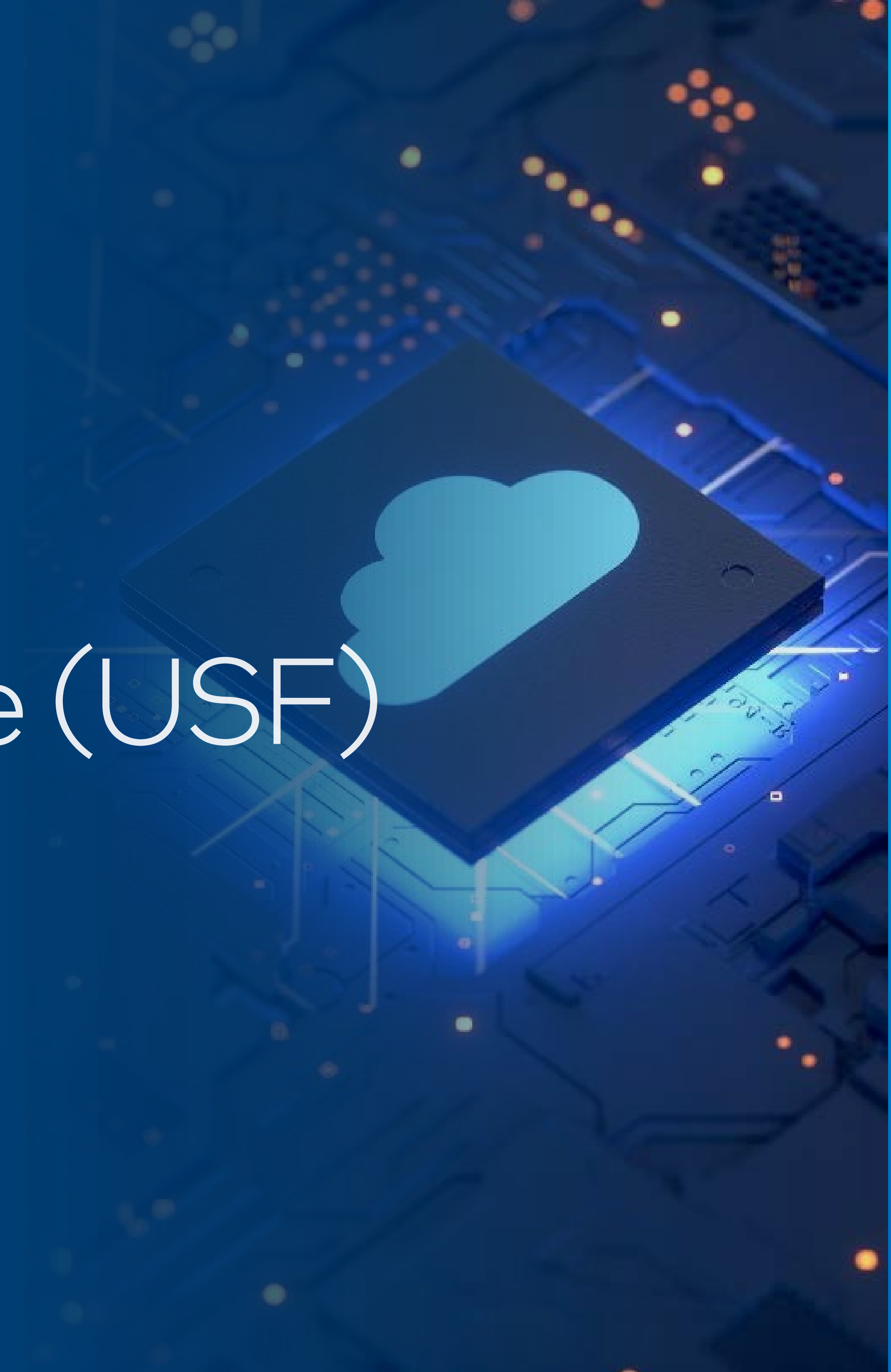
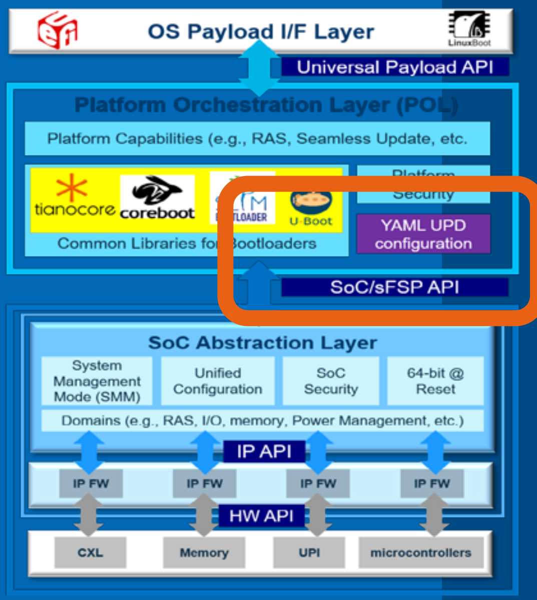
System Firmware Training

Universal Scalable Firmware (USF) Configuration Data

Intel Corporation





Configuration Region

Updatable Product Data (UPD) – Defaults for Scalable Intel FSP Initialization

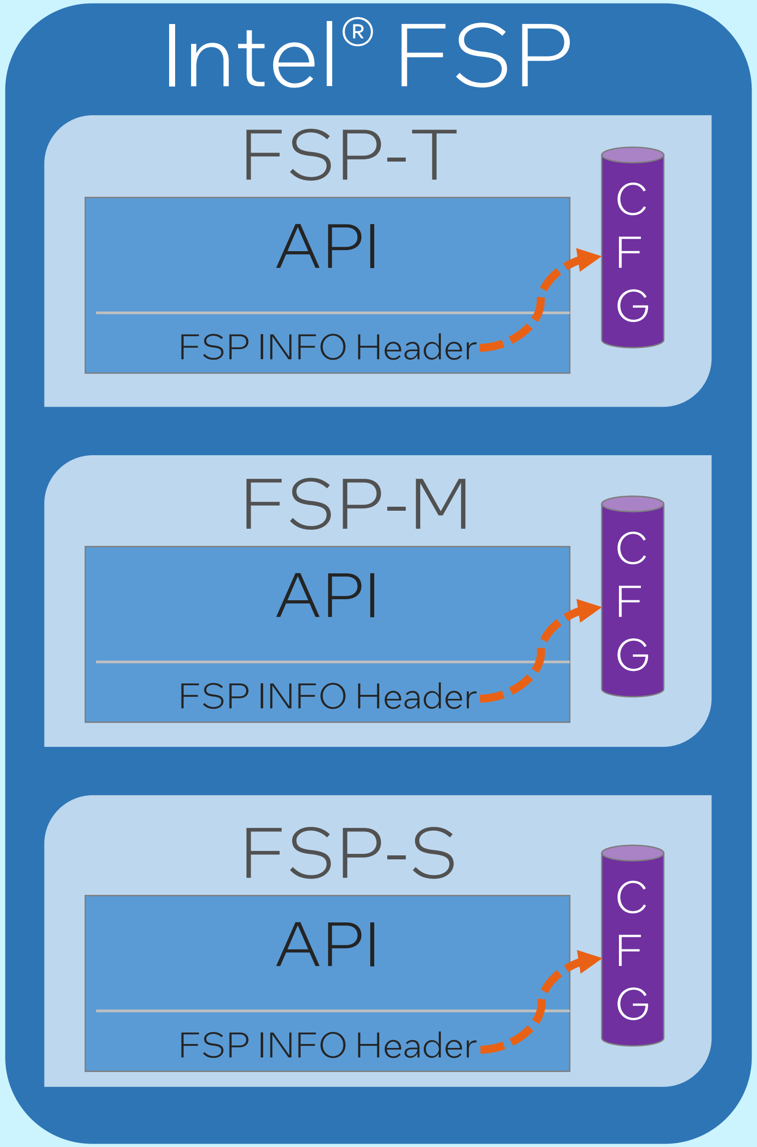
The Intel® Firmware Support Package Includes

- A binary firmware device (FD) file - contains multiple FSP Modules
- An integration guide
- A rebasing tool
- A Boot Setting File (BSF) or YAML file for Configuration of the Updatable Product Data (UPD)

Intel® FSP V2.3 Binary Component View

Layout of the Intel FSP Binary

- Each FV has Configuration Region - Updatable Product Data (UPD) and is unique
- **Runtime** Bootloader accesses during PI
  - FSP-T: Temporary RAM initialization phase
    - `File: FsptUpd.h`
  - FSP-M: Memory initialization phase
    - `File: FspmUpd.h`
  - FSP-S: Silicon initialization phase
    - `File: FspmUpd.h`
- **Build time** configuration done using Binary Configuration Tool (BCT) or open source YAML configuration tool



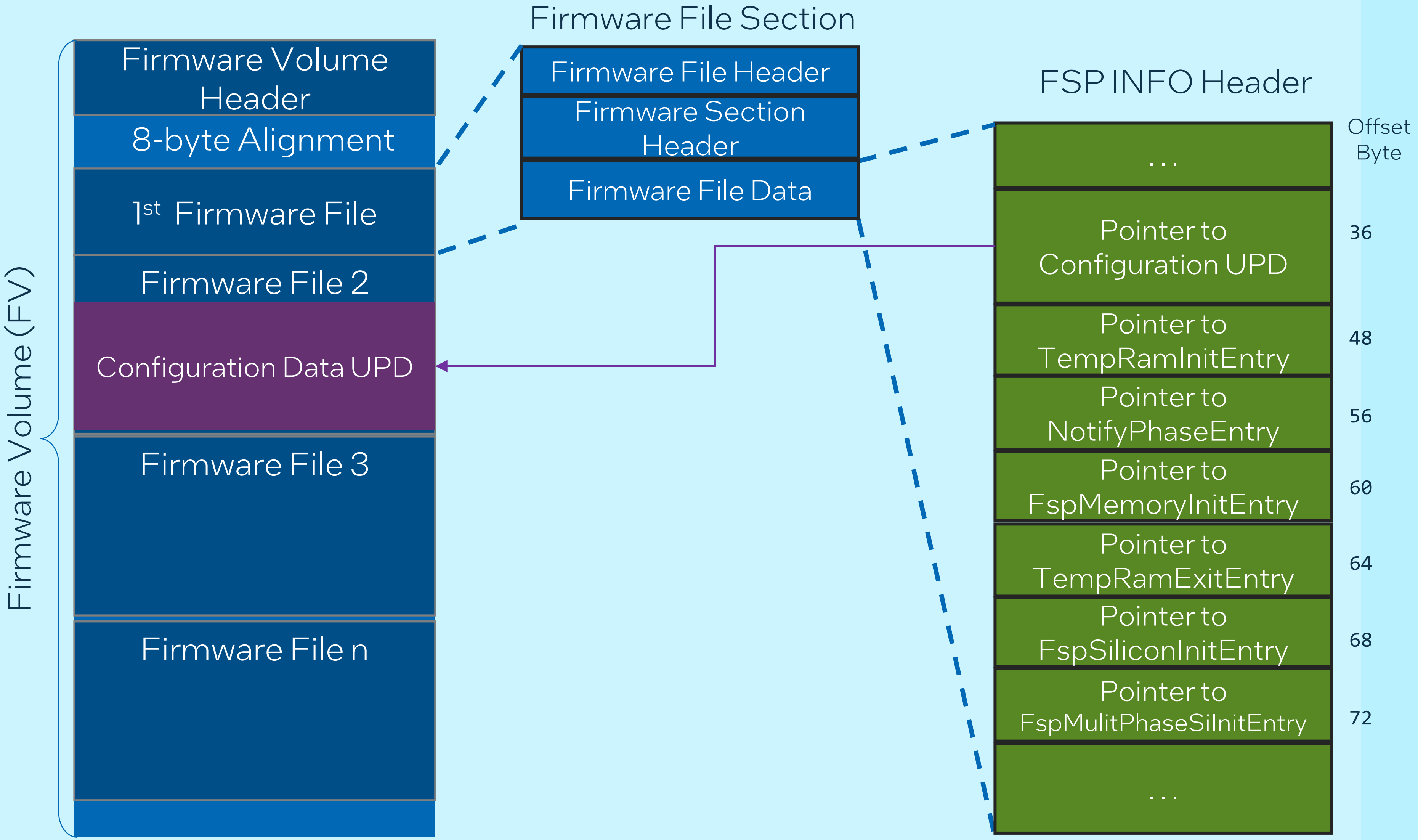
Intel® FSP Spec 2.3 Figure 1

Intel® FSP Binary Structure FSP_INFO_HEADER UPD

FSP INFO Header is the first Firmware File within each of the FSP Component's FV

Each FSP (FV) contains a configurable data region (UPD) which is used by the FSP during initialization

Note: If a pointer in the FSP INFO Header is 0x00000000 then API not available in this component



Intel® FSP Spec 2.3 Table 1

Static / Build Time Configuration

Tools

- YAML Python Config Editor
- Binary Configuration Tool (BCT)

How to Edit the UPD Config in Intel® FSP Binary

YAML UPD Config Editor

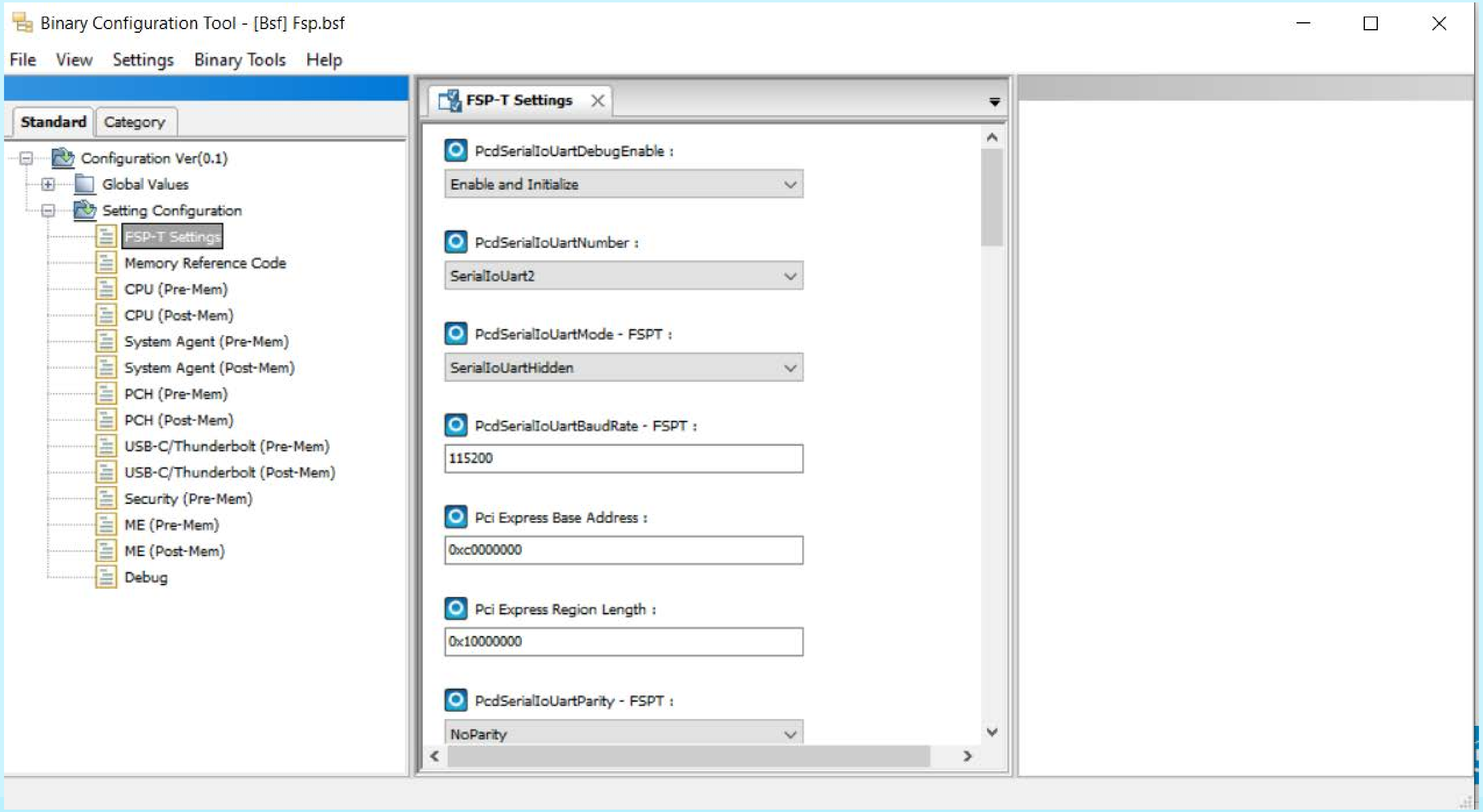
- DSC, DEC, VFR, UNI, HFR, BSF, PCD -> YAML to enable single data source, compared to many places to change for configuration
- Streamline configuration process across UEFI and bootloaders.
- Open-source Config Editor tool support, https://github.com/tianocore/edk2/tree/master/IntelFsp2Pkg/Tools/ConfigEditor

Binary Configuration Tool (BCT)

- Closed source
- Boot Settings File (BSF) Specification https://software.intel.com/en-us/download/boot-setting-file-specification-release-10
- Link to tool: https://github.com/intel/BCT

Binary Setting File and Binary Configuration Tool

https://github.com/intel/BCT



FSP-T Settings

PcdSerialIoUartDebugEnable : Enable and Initialize

PcdSerialIoUartNumber : SerialIoUart2

PcdSerialIoUartMode - FSPT : SerialIoUartHidden

PcdSerialIoUartBaudRate - FSPT : 115200

Pci Express Base Address : 0xc0000000

Pci Express Region Length : 0x10000000

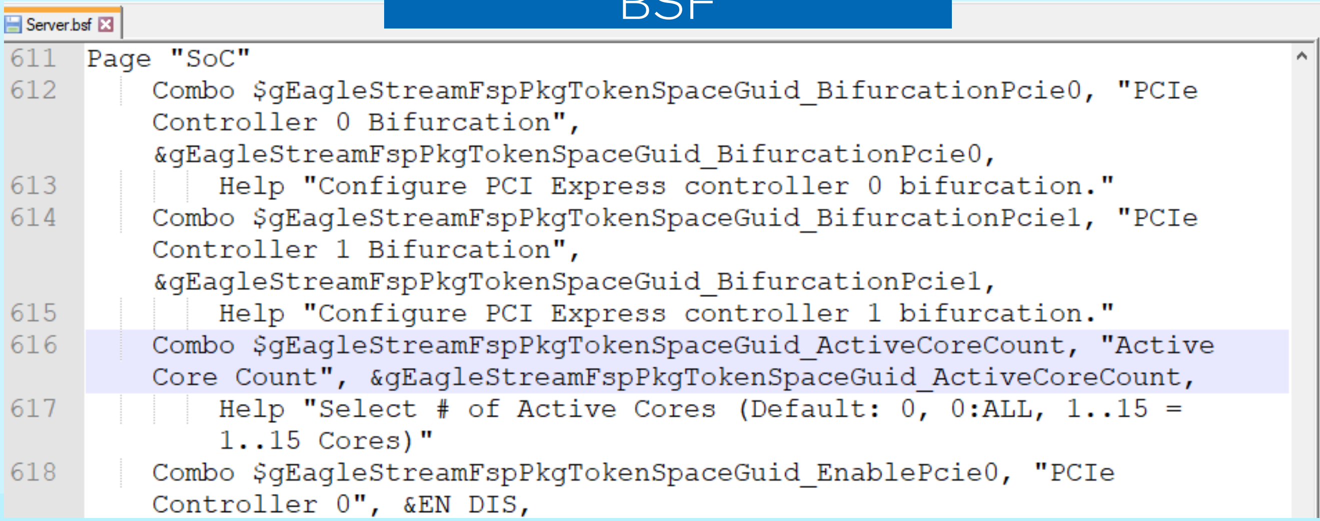
PcdSerialIoUartParity - FSPT : NoParity

Comparison between BSF and YAML

What is YAML?

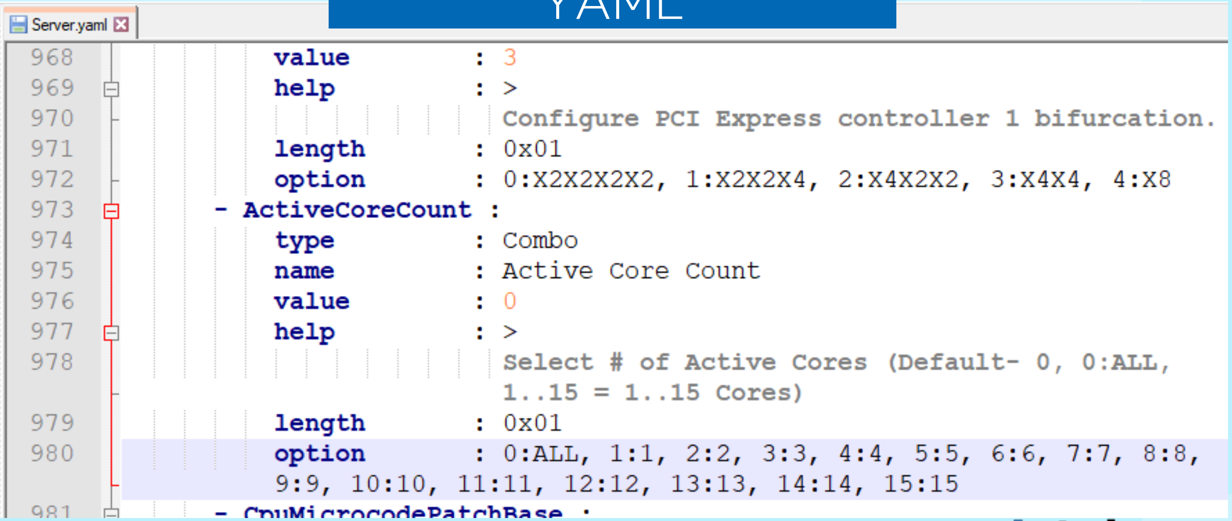
- Human-readable data-serialization language
- List of key/value pairs. Superset of JSON.
- 19 years of history, widely adopted. Many tools/libraries available.
- Slim bootloader currently using YAML as single configuration source

BSF



```
Page "SoC"
    Combo $gEagleStreamFspPkgTokenSpaceGuid_BifurcationPcie0, "PCIe
    Controller 0 Bifurcation",
    &gEagleStreamFspPkgTokenSpaceGuid_BifurcationPcie0,
        Help "Configure PCI Express controller 0 bifurcation."
    Combo $gEagleStreamFspPkgTokenSpaceGuid_BifurcationPcie1, "PCIe
    Controller 1 Bifurcation",
    &gEagleStreamFspPkgTokenSpaceGuid_BifurcationPcie1,
        Help "Configure PCI Express controller 1 bifurcation."
    Combo $gEagleStreamFspPkgTokenSpaceGuid_ActiveCoreCount, "Active
    Core Count", &gEagleStreamFspPkgTokenSpaceGuid_ActiveCoreCount,
        Help "Select # of Active Cores (Default: 0, 0:ALL, 1..15 =
        1..15 Cores)"
    Combo $gEagleStreamFspPkgTokenSpaceGuid_EnablePcie0, "PCIe
    Controller 0", &EN DIS,
```

YAML

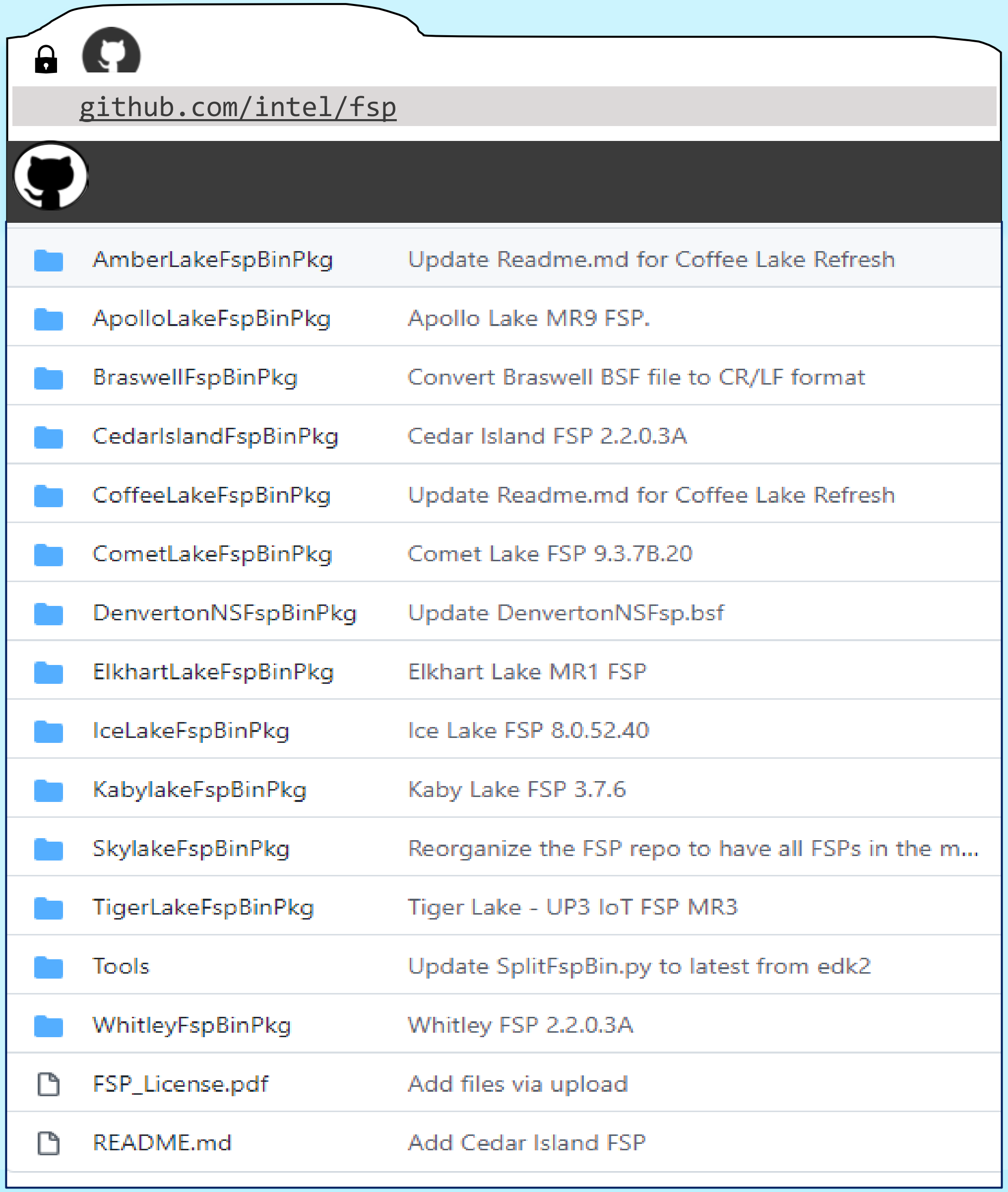


```
          value            : 3
          help             : >
                             Configure PCI Express controller 1 bifurcation.
          length           : 0x01
          option           : 0:X2X2X2X2, 1:X2X2X4, 2:X4X2X2, 3:X4X4, 4:X8
      - ActiveCoreCount :
          type             : Combo
          name             : Active Core Count
          value            : 0
          help             : >
                             Select # of Active Cores (Default- 0, 0:ALL,
                             1..15 = 1..15 Cores)
          length           : 0x01
          option           : 0:ALL, 1:1, 2:2, 3:3, 4:4, 5:5, 6:6, 7:7, 8:8,
          9:9, 10:10, 11:11, 12:12, 13:13, 14:14, 15:15
      - CpuMicrocodePatchBase :
```

YAML Config Tool for Intel® FSP UPD

YAML UPD Editor Features:

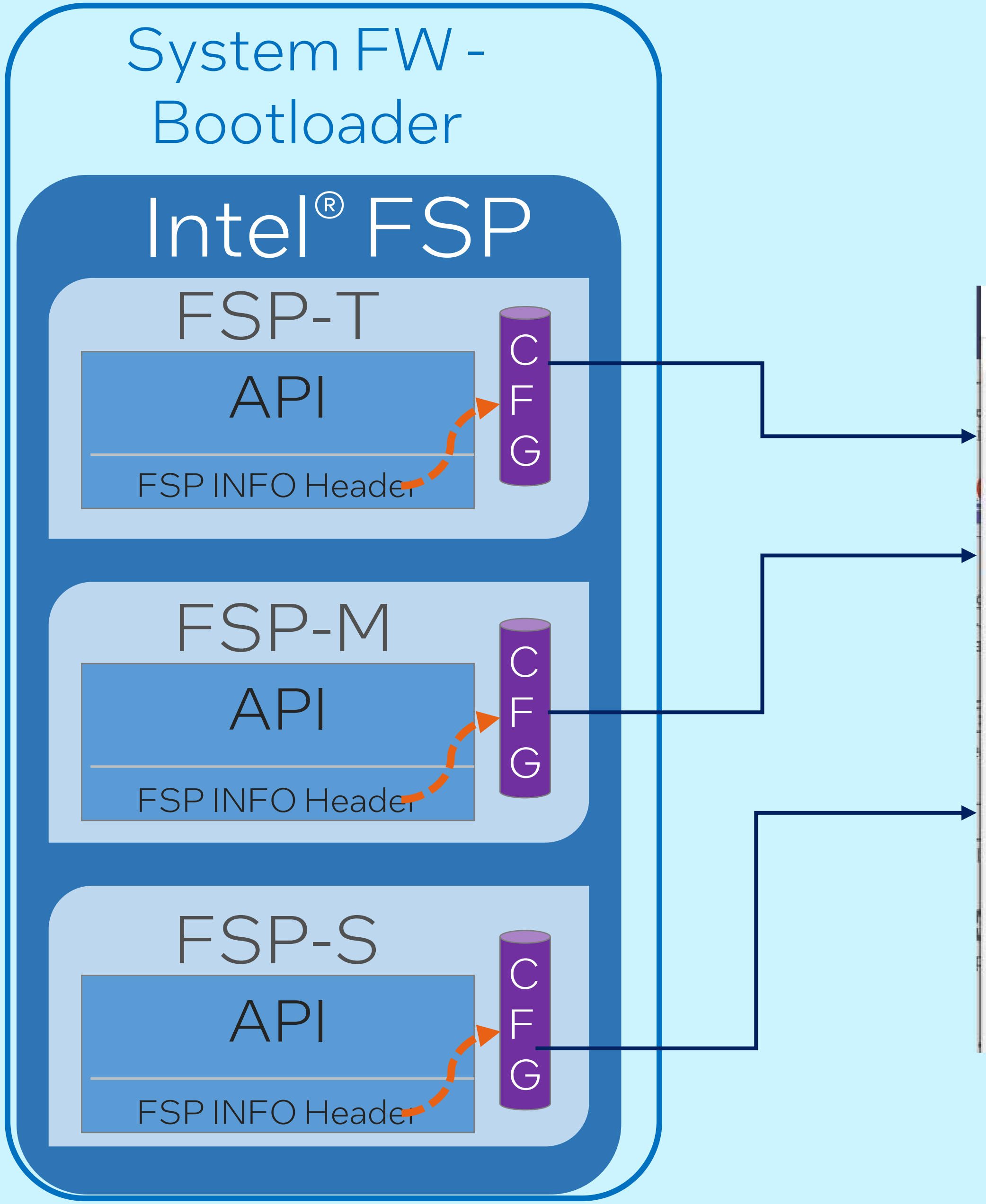
- Read FSP binary information
- Allow patching any BIOS/IFWI image containing FSP UPDs
- Read YAML config format while BSF backward compatible
- Bit format FSP support instead of bytes
- Modifying BSF parameters and export loadable delta files
- FSP 1.x and 2.x format backward compatible
- Search function



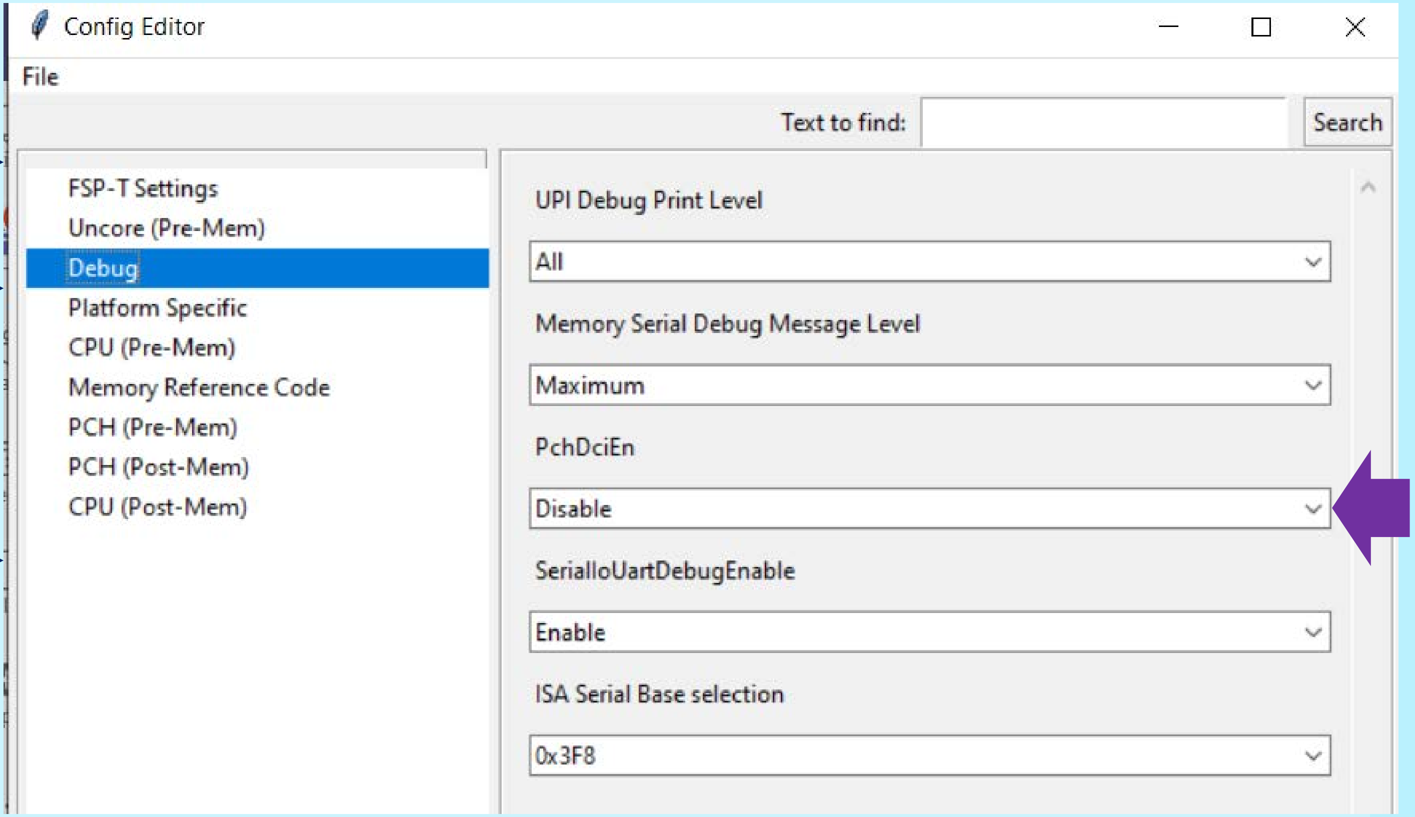
github.com/intel/fsp

AmberLakeFspBinPkg	Update Readme.md for Coffee Lake Refresh
ApolloLakeFspBinPkg	Apollo Lake MR9 FSP.
BraswellFspBinPkg	Convert Braswell BSF file to CR/LF format
CedarIslandFspBinPkg	Cedar Island FSP 2.2.0.3A
CoffeeLakeFspBinPkg	Update Readme.md for Coffee Lake Refresh
CometLakeFspBinPkg	Comet Lake FSP 9.3.7B.20
DenvertonNSFspBinPkg	Update DenvertonNSFsp.bsf
ElkhartLakeFspBinPkg	Elkhart Lake MR1 FSP
IceLakeFspBinPkg	Ice Lake FSP 8.0.52.40
KabylakeFspBinPkg	Kaby Lake FSP 3.7.6
SkylakeFspBinPkg	Reorganize the FSP repo to have all FSPs in the m...
TigerLakeFspBinPkg	Tiger Lake - UP3 IoT FSP MR3
Tools	Update SplitFspBin.py to latest from edk2
WhitleyFspBinPkg	Whitley FSP 2.2.0.3A
FSP_License.pdf	Add files via upload
README.md	Add Cedar Island FSP

YAML Editor Reads Config file



Intel® FSP Spec 2.3 Figure 1



UPI Debug Print Level: All

Memory Serial Debug Message Level: Maximum

PchDciEn: Disable

SerialIoUartDebugEnable: Enable

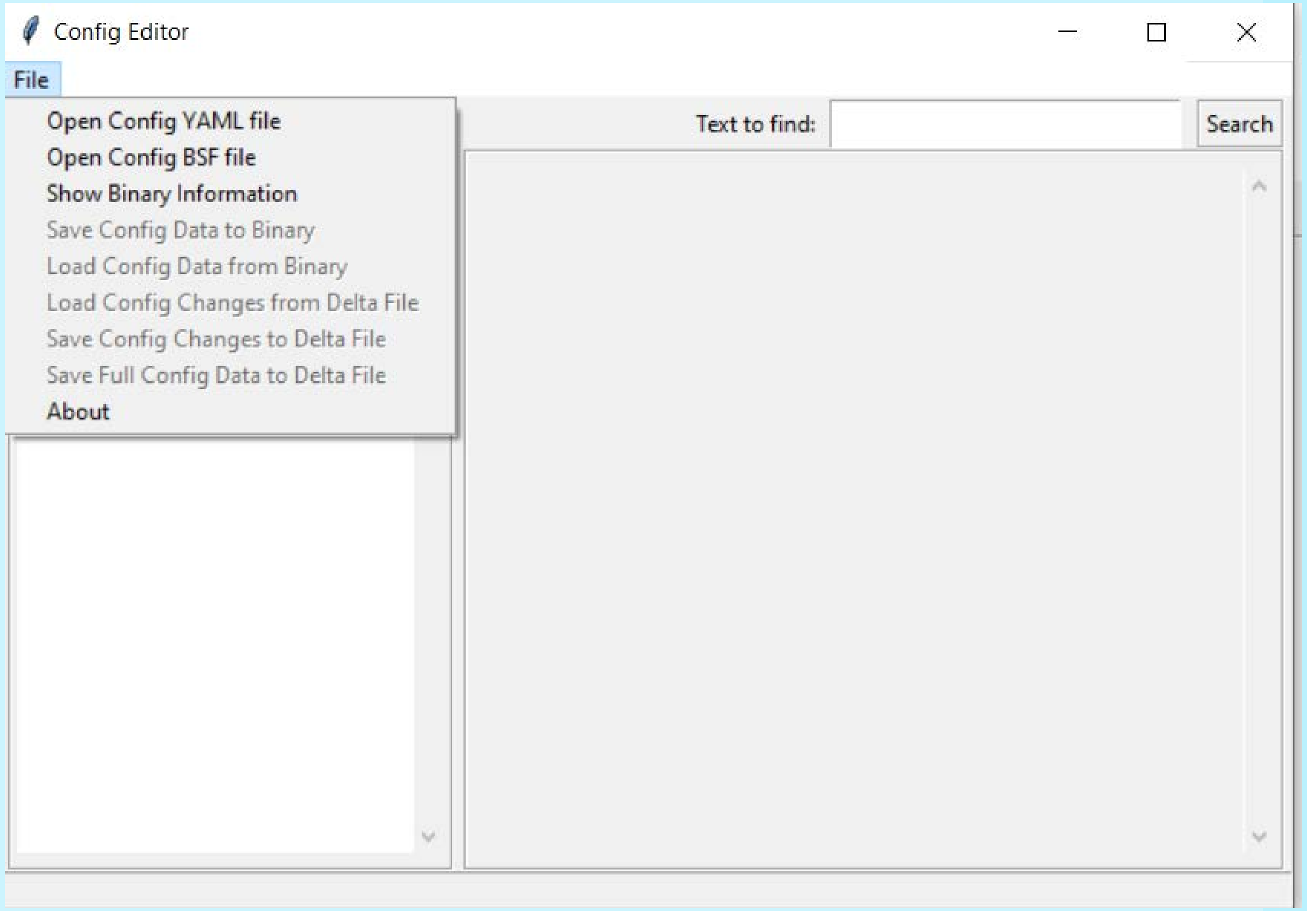
ISA Serial Base selection: 0x3F8

YAML Configuration Editor

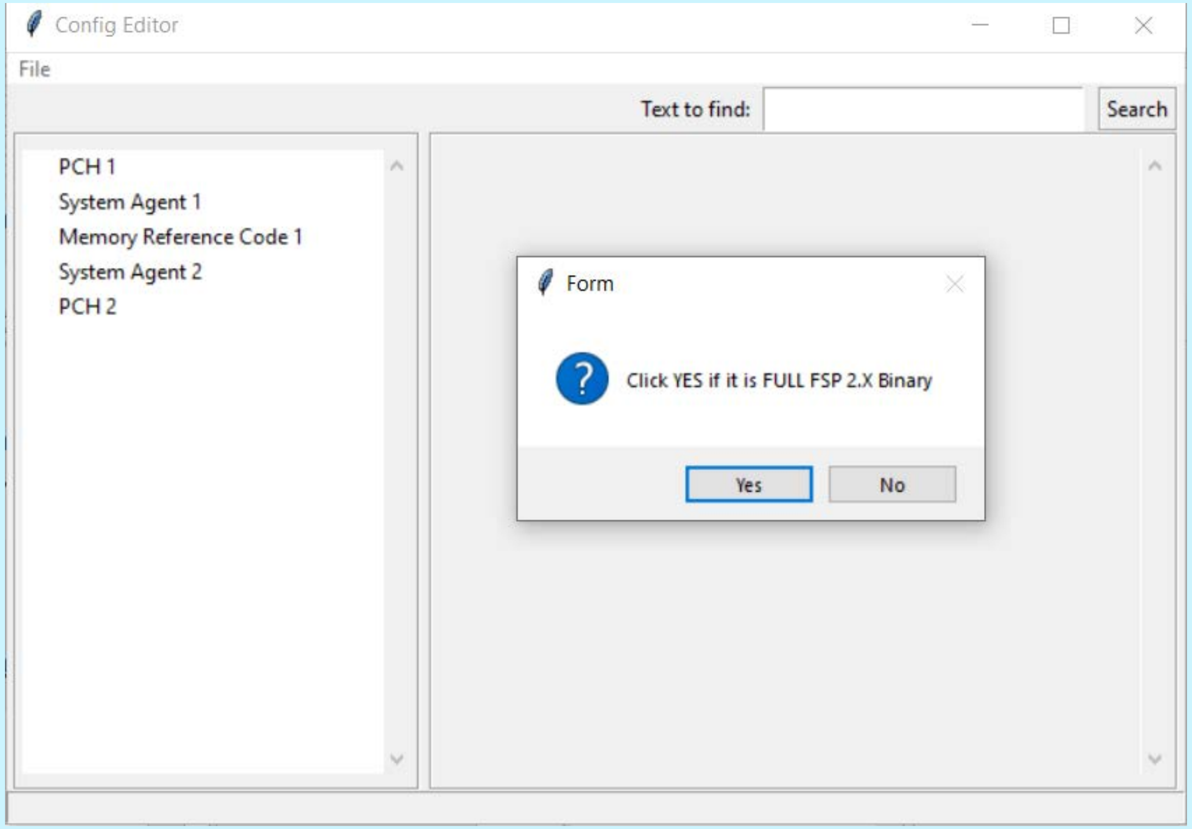
UPD Config Editor Interfaces

Steps to run

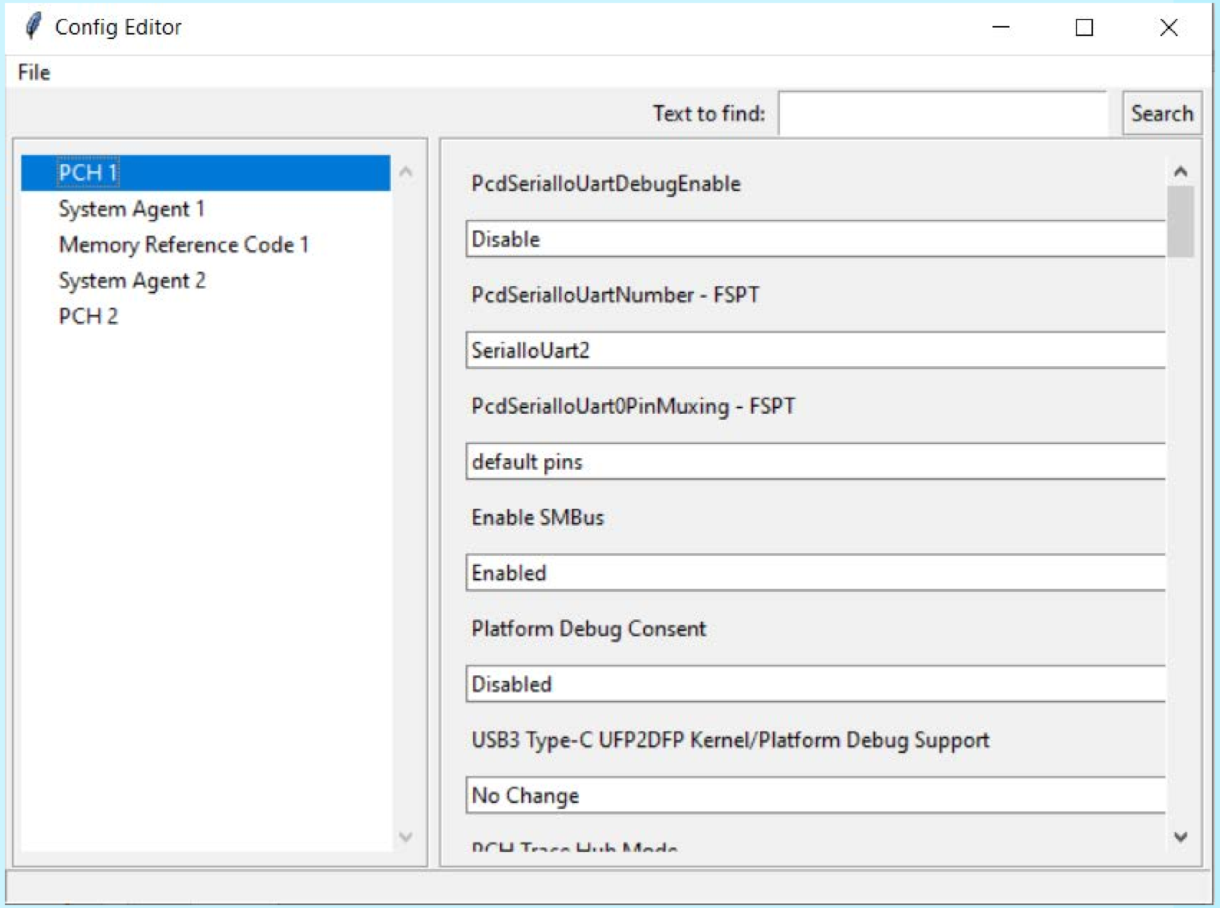
- Clone Intel FSP at https://github.com/intel/FSP
- Clone edk2 code at https://github.com/tianocore/edk2
- ConfigEditor is located at IntelFsp2Pkg/Tools/ConfigEditor
- Run "python ConfigEditor.py"


Config Editor
File
Open Config YAML file
Open Config BSF file
Show Binary Information
Save Config Data to Binary
Load Config Data from Binary
Load Config Changes from Delta File
Save Config Changes to Delta File
Save Full Config Data to Delta File
About
Text to find:
Search

Load BSF file



Click YES if it is FULL FSP 2.X Binary



PcdSerialIoUartDebugEnable

Disable

PcdSerialIoUartNumber - FSPT

SerialIoUart2

PcdSerialIoUart0PinMuxing - FSPT

default pins

Enable SMBus

Enabled

Platform Debug Consent

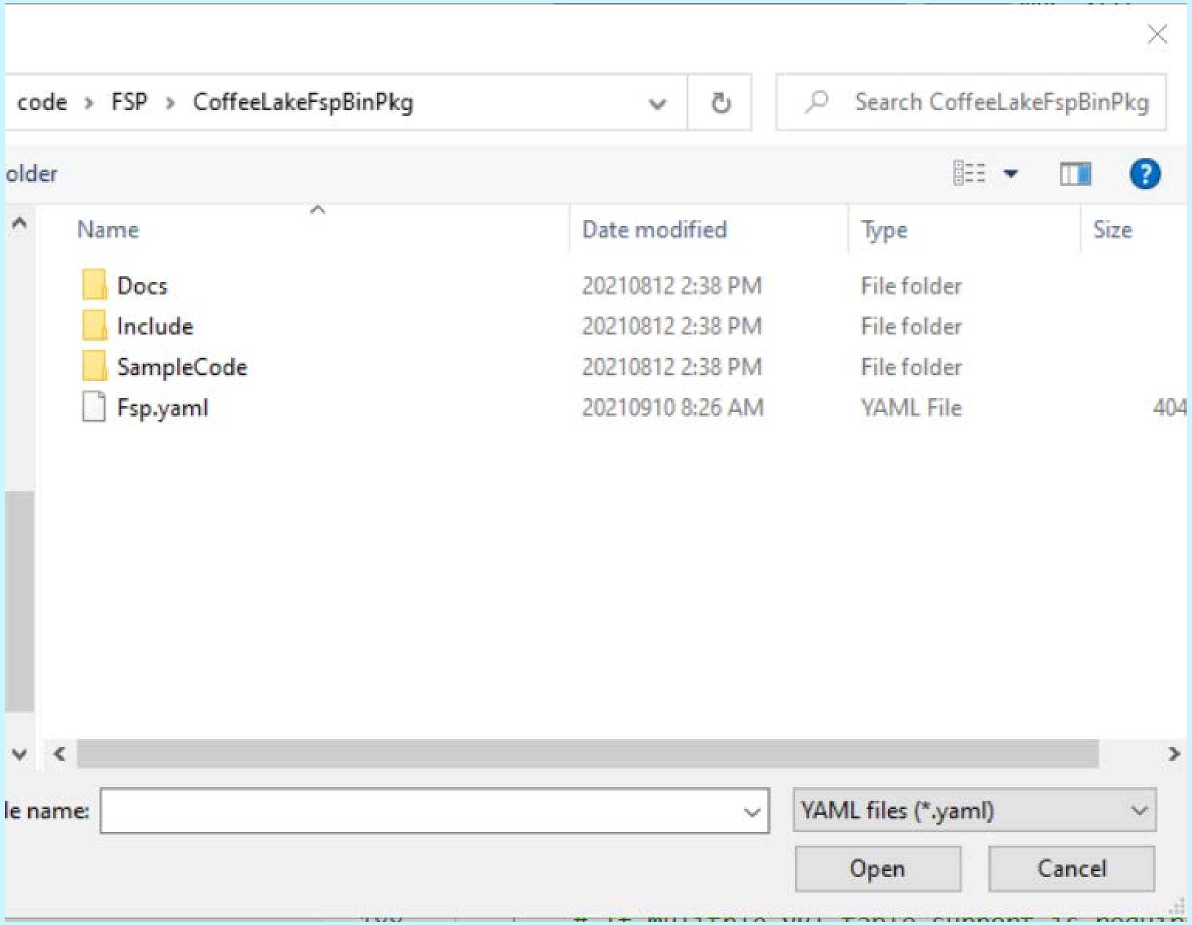
Disabled

USB3 Type-C UFP2DFP Kernel/Platform Debug Support

No Change

PCH Trace Hub Mode

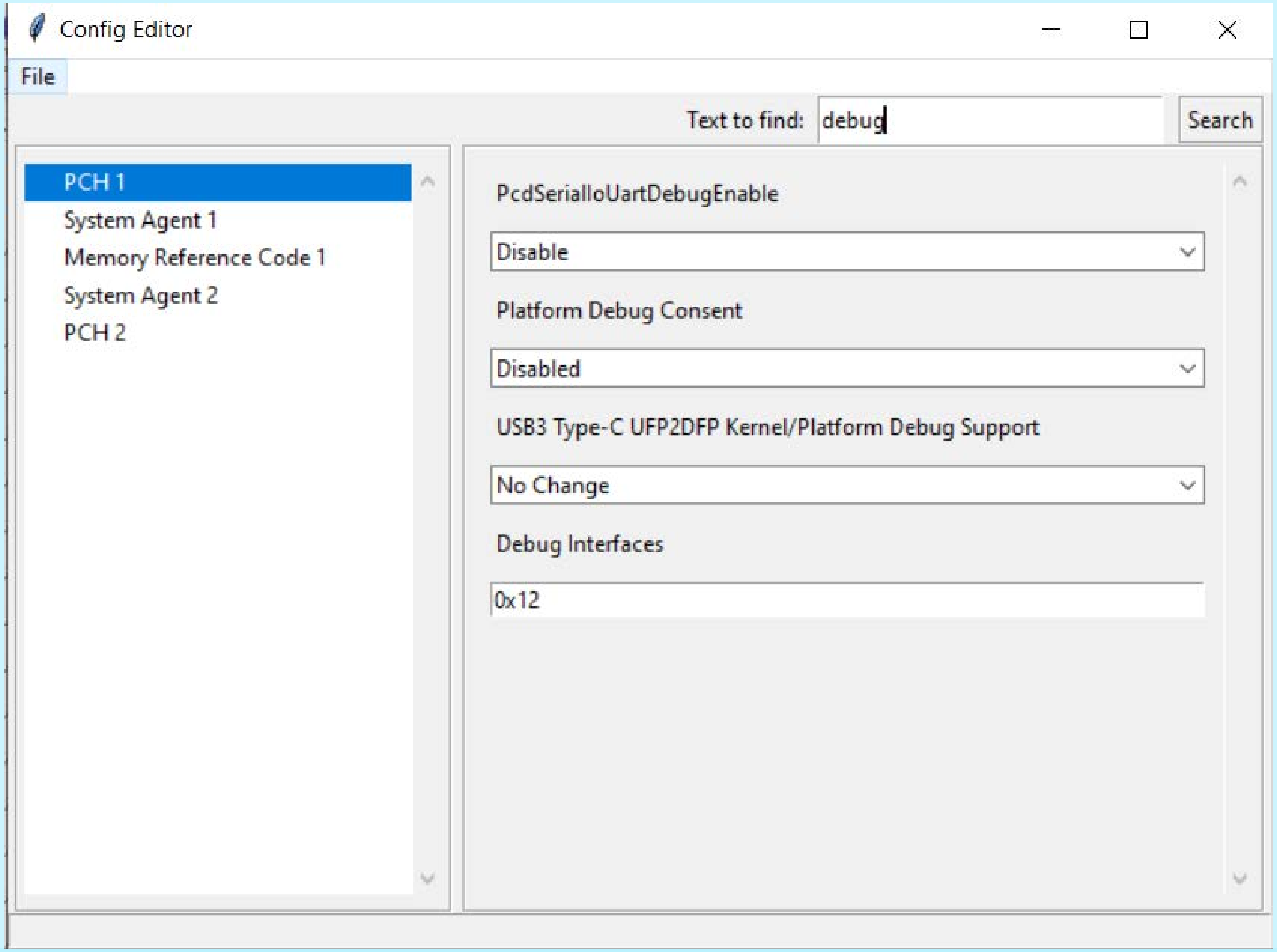
After loading BSF, a YAML file will be generated.



Name	Date modified	Type	Size
Docs	20210812 2:38 PM	File folder	
Include	20210812 2:38 PM	File folder	
SampleCode	20210812 2:38 PM	File folder	
Fsp.yaml	20210910 8:26 AM	YAML File	404

- YAML file can also be generated during BIOS build process using
- FspDscBsf2Yaml.py
- utility in https://github.com/tianocore/edk2/blob/master/IntelFsp2Pkg/Tools/FspDscBsf2Yaml.py

An additional search function



Text to find: debug

PcdSerialIoUartDebugEnable

Disable

Platform Debug Consent

Disabled

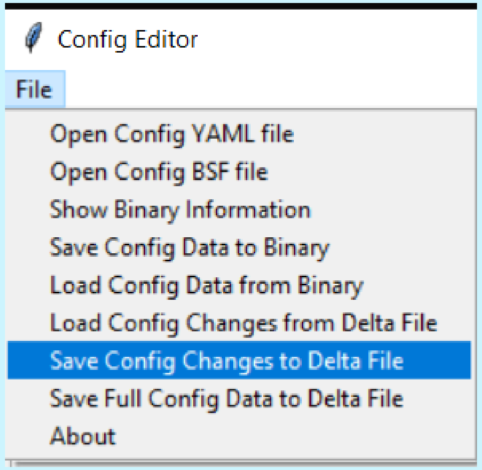
USB3 Type-C UFP2DFP Kernel/Platform Debug Support

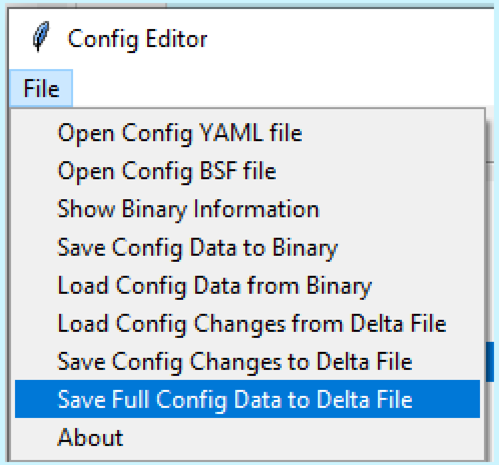
No Change

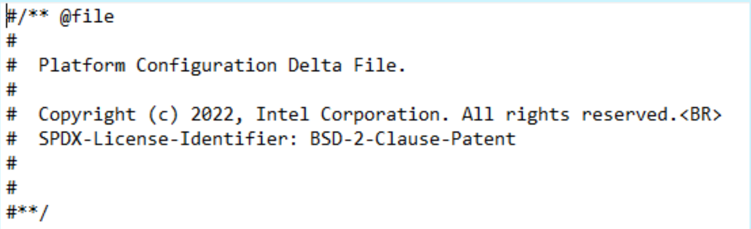
Debug Interfaces

0x12

Able to generate delta file to track changes

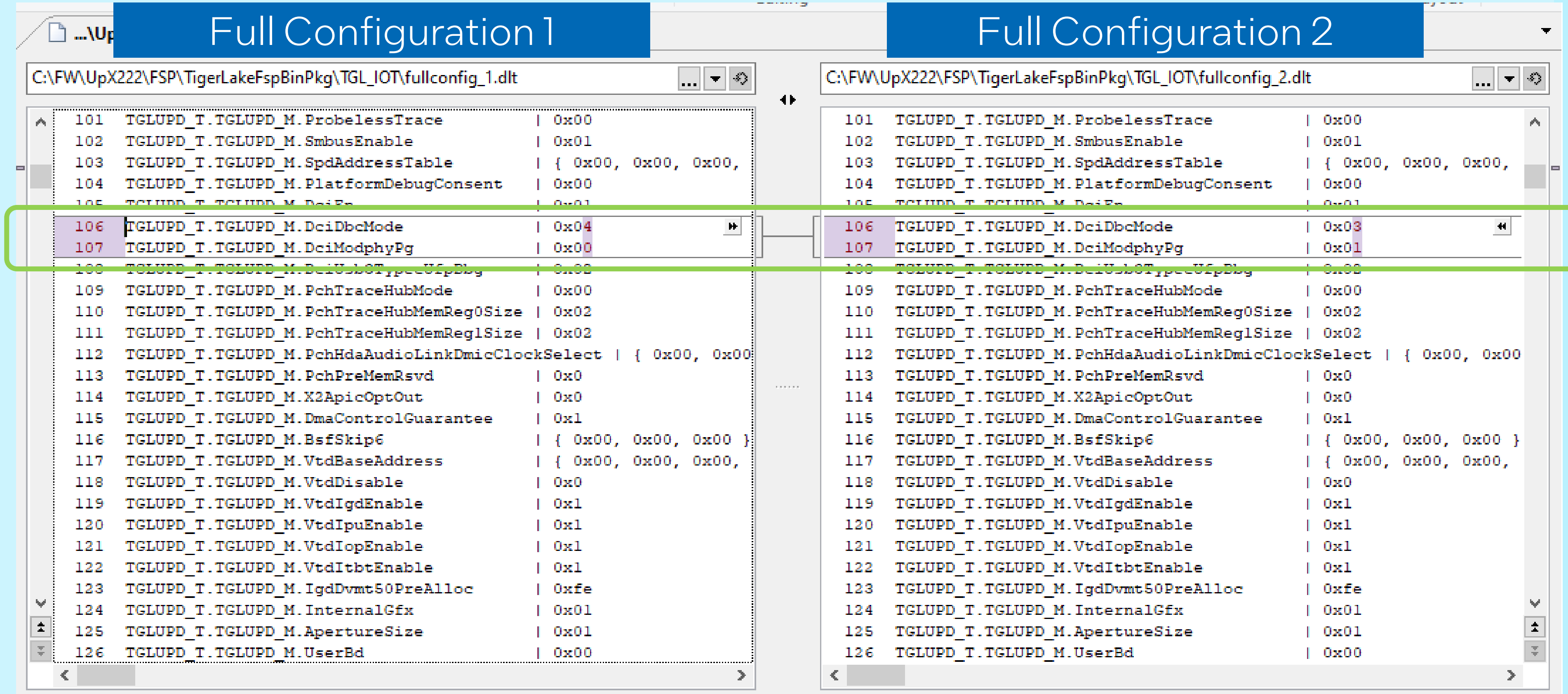

Config Editor
File
Open Config YAML file
Open Config BSF file
Show Binary Information
Save Config Data to Binary
Load Config Data from Binary
Load Config Changes from Delta File
Save Config Changes to Delta File
Save Full Config Data to Delta File
About


Config Editor
File
Open Config YAML file
Open Config BSF file
Show Binary Information
Save Config Data to Binary
Load Config Data from Binary
Load Config Changes from Delta File
Save Config Changes to Delta File
Save Full Config Data to Delta File
About



```
#/** @file
#
#  Platform Configuration Delta File.
#
#  Copyright (c) 2022, Intel Corporation. All rights reserved.<BR>
#  SPDX-License-Identifier: BSD-2-Clause-Patent
#
#
#**/
```

Differences



Full Configuration 1

C:\FW\UpX222\FSP\TigerLakeFspBinPkg\TGL_IOT\fullconfig_1.dlt

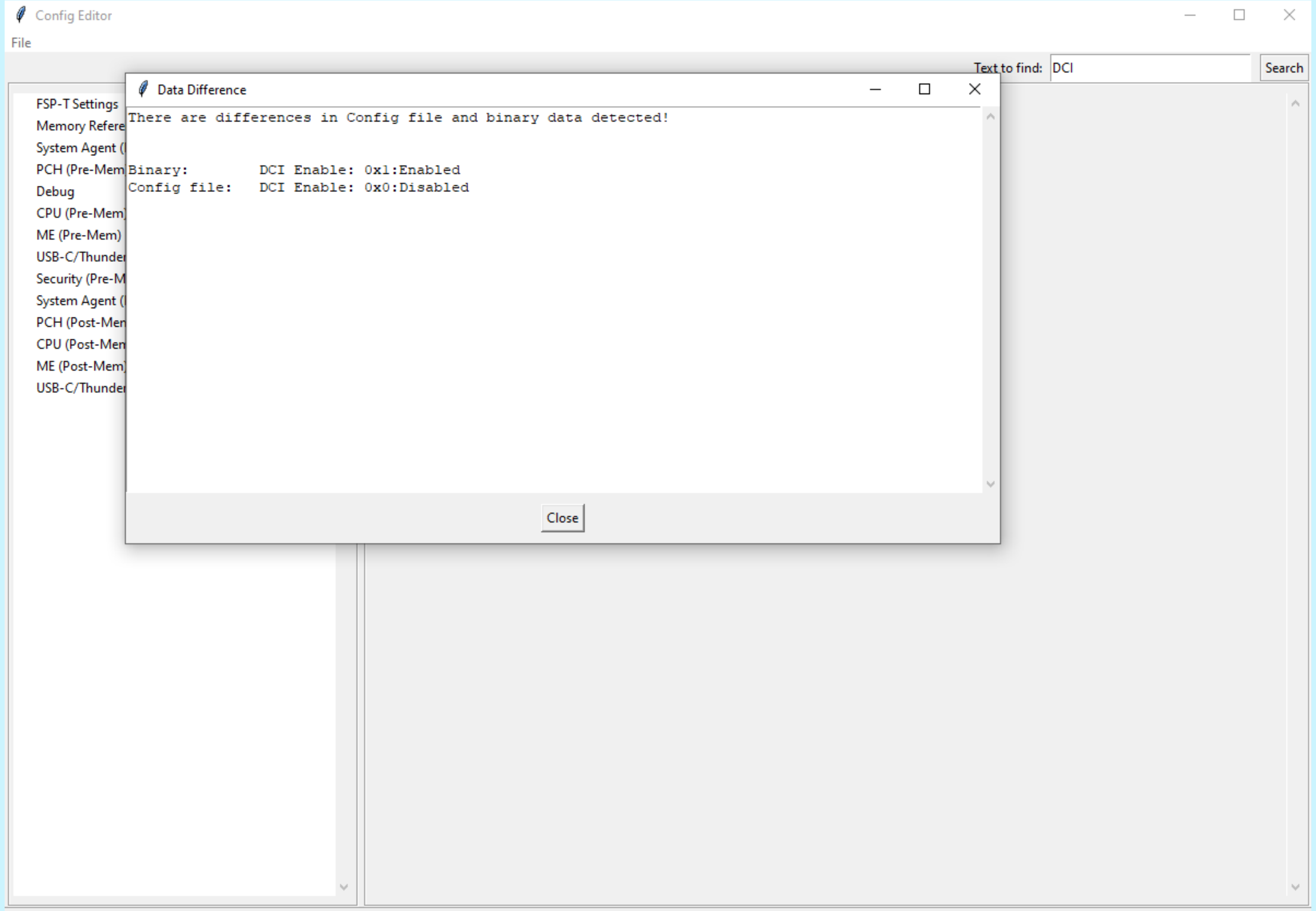
```
TGLUPD_T.TGLUPD_M.ProbelessTrace              | 0x00
TGLUPD_T.TGLUPD_M.SmbusEnable                 | 0x01
TGLUPD_T.TGLUPD_M.SpdAddressTable             | { 0x00, 0x00, 0x00,
TGLUPD_T.TGLUPD_M.PlatformDebugConsent        | 0x00
TGLUPD_T.TGLUPD_M.DciEn                       | 0x01
TGLUPD_T.TGLUPD_M.DciDbcMode                  | 0x04
TGLUPD_T.TGLUPD_M.DciModphyPg                 | 0x00
TGLUPD_T.TGLUPD_M.DciUsb3TypecUfpDbg          | 0x02
TGLUPD_T.TGLUPD_M.PchTraceHubMode             | 0x00
TGLUPD_T.TGLUPD_M.PchTraceHubMemReg0Size      | 0x02
TGLUPD_T.TGLUPD_M.PchTraceHubMemReg1Size      | 0x02
TGLUPD_T.TGLUPD_M.PchHdaAudioLinkDmicClockSelect | { 0x00, 0x00
TGLUPD_T.TGLUPD_M.PchPreMemRsvd               | 0x0
TGLUPD_T.TGLUPD_M.X2ApicOptOut                | 0x0
TGLUPD_T.TGLUPD_M.DmaControlGuarantee         | 0x1
TGLUPD_T.TGLUPD_M.BsfSkip6                    | { 0x00, 0x00, 0x00 }
TGLUPD_T.TGLUPD_M.VtdBaseAddress              | { 0x00, 0x00, 0x00,
TGLUPD_T.TGLUPD_M.VtdDisable                  | 0x0
TGLUPD_T.TGLUPD_M.VtdIgdEnable                | 0x1
TGLUPD_T.TGLUPD_M.VtdIpuEnable                | 0x1
TGLUPD_T.TGLUPD_M.VtdIopEnable                | 0x1
TGLUPD_T.TGLUPD_M.VtdItbtEnable               | 0x1
TGLUPD_T.TGLUPD_M.IgdDvmt50PreAlloc           | 0xfe
TGLUPD_T.TGLUPD_M.InternalGfx                 | 0x01
TGLUPD_T.TGLUPD_M.ApertureSize                | 0x01
TGLUPD_T.TGLUPD_M.UserBd                      | 0x00
```

Full Configuration 2

C:\FW\UpX222\FSP\TigerLakeFspBinPkg\TGL_IOT\fullconfig_2.dlt

```
TGLUPD_T.TGLUPD_M.ProbelessTrace              | 0x00
TGLUPD_T.TGLUPD_M.SmbusEnable                 | 0x01
TGLUPD_T.TGLUPD_M.SpdAddressTable             | { 0x00, 0x00, 0x00,
TGLUPD_T.TGLUPD_M.PlatformDebugConsent        | 0x00
TGLUPD_T.TGLUPD_M.DciEn                       | 0x01
TGLUPD_T.TGLUPD_M.DciDbcMode                  | 0x03
TGLUPD_T.TGLUPD_M.DciModphyPg                 | 0x01
TGLUPD_T.TGLUPD_M.DciUsb3TypecUfpDbg          | 0x02
TGLUPD_T.TGLUPD_M.PchTraceHubMode             | 0x00
TGLUPD_T.TGLUPD_M.PchTraceHubMemReg0Size      | 0x02
TGLUPD_T.TGLUPD_M.PchTraceHubMemReg1Size      | 0x02
TGLUPD_T.TGLUPD_M.PchHdaAudioLinkDmicClockSelect | { 0x00, 0x00
TGLUPD_T.TGLUPD_M.PchPreMemRsvd               | 0x0
TGLUPD_T.TGLUPD_M.X2ApicOptOut                | 0x0
TGLUPD_T.TGLUPD_M.DmaControlGuarantee         | 0x1
TGLUPD_T.TGLUPD_M.BsfSkip6                    | { 0x00, 0x00, 0x00 }
TGLUPD_T.TGLUPD_M.VtdBaseAddress              | { 0x00, 0x00, 0x00,
TGLUPD_T.TGLUPD_M.VtdDisable                  | 0x0
TGLUPD_T.TGLUPD_M.VtdIgdEnable                | 0x1
TGLUPD_T.TGLUPD_M.VtdIpuEnable                | 0x1
TGLUPD_T.TGLUPD_M.VtdIopEnable                | 0x1
TGLUPD_T.TGLUPD_M.VtdItbtEnable               | 0x1
TGLUPD_T.TGLUPD_M.IgdDvmt50PreAlloc           | 0xfe
TGLUPD_T.TGLUPD_M.InternalGfx                 | 0x01
TGLUPD_T.TGLUPD_M.ApertureSize                | 0x01
TGLUPD_T.TGLUPD_M.UserBd                      | 0x00
```

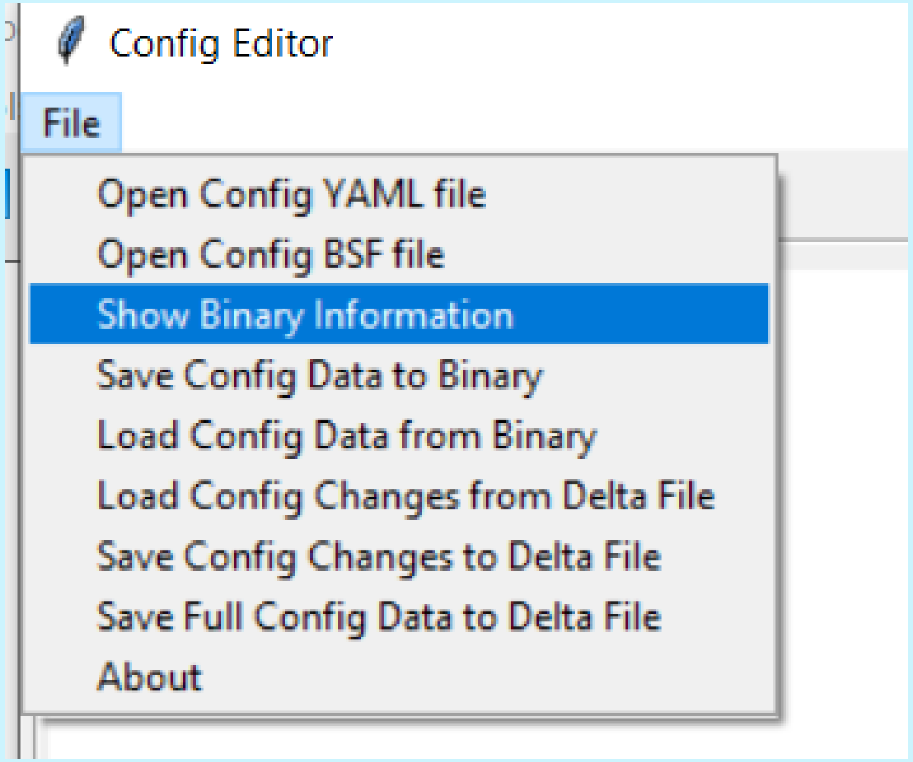
Detect difference in config file and binary

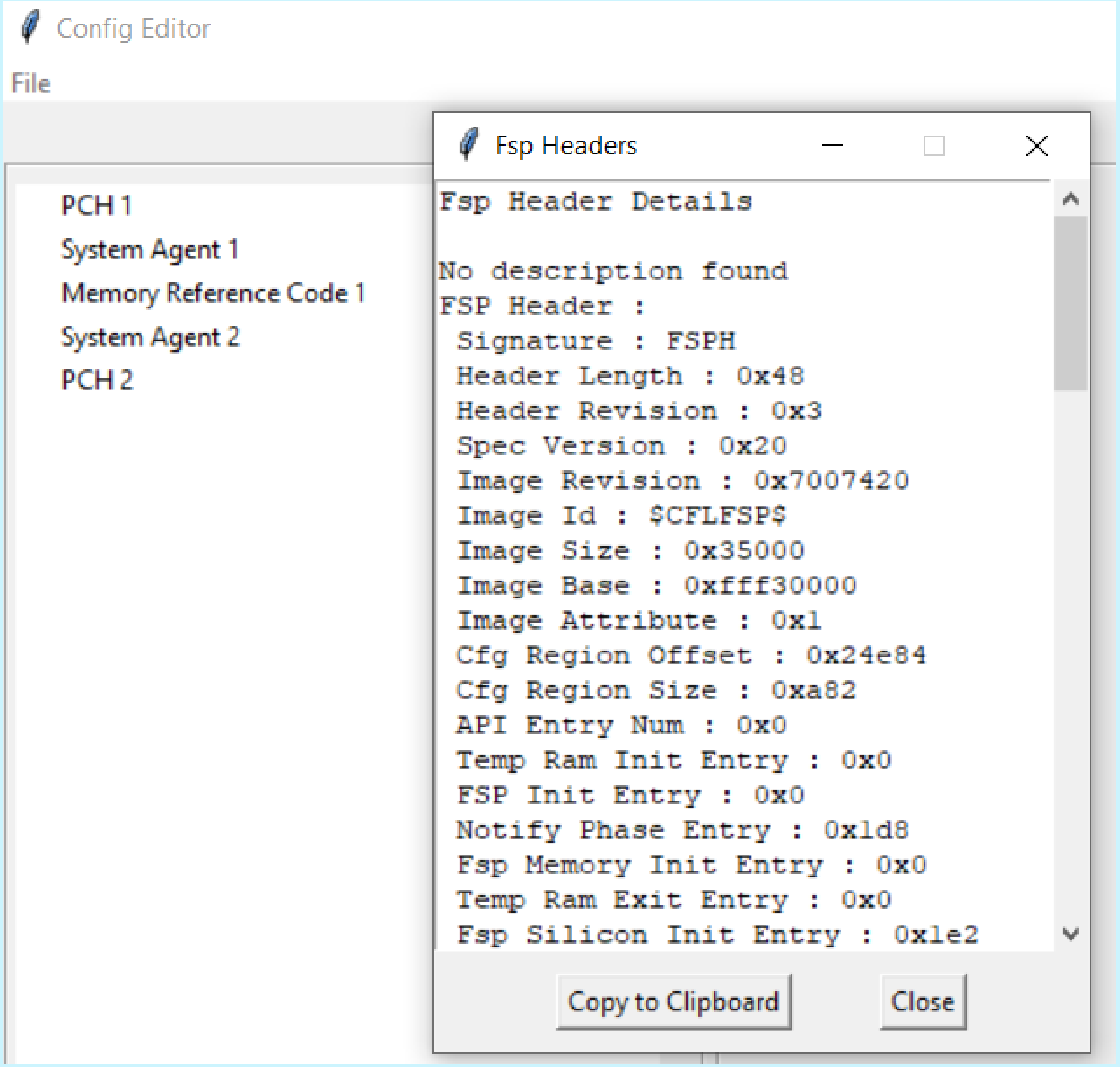


```
There are differences in Config file and binary data detected!


Binary:        DCI Enable: 0x1:Enabled
Config file:   DCI Enable: 0x0:Disabled
```

- Load BSF or YAML file
- Load a modified binary file
- A pop up will appear describing the differences.

Show binary information


Config Editor
File
Open Config YAML file
Open Config BSF file
Show Binary Information
Save Config Data to Binary
Load Config Data from Binary
Load Config Changes from Delta File
Save Config Changes to Delta File
Save Full Config Data to Delta File
About



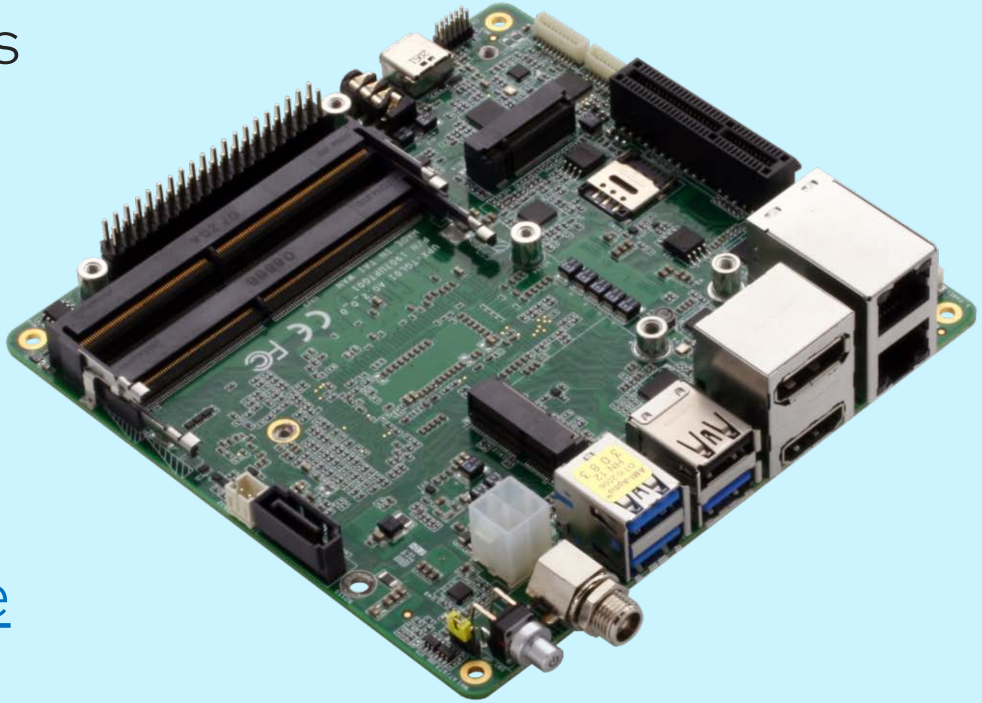
```
Fsp Header Details

No description found
FSP Header :
 Signature : FSPH
 Header Length : 0x48
 Header Revision : 0x3
 Spec Version : 0x20
 Image Revision : 0x7007420
 Image Id : $CFLFSP$
 Image Size : 0x35000
 Image Base : 0xfff30000
 Image Attribute : 0x1
 Cfg Region Offset : 0x24e84
 Cfg Region Size : 0xa82
 API Entry Num : 0x0
 Temp Ram Init Entry : 0x0
 FSP Init Entry : 0x0
 Notify Phase Entry : 0x1d8
 Fsp Memory Init Entry : 0x0
 Temp Ram Exit Entry : 0x0
 Fsp Silicon Init Entry : 0x1e2
```

Flash Binary Image onto SUT

- Board:
- The UP Xtreme i11 board (UP Xtreme i11) is an x86 maker board based on Intel platform Tiger Lake UP3, used in IoT, industrial automation, digital signage areas, etc.
- https://up-shop.org/up-xtreme-i11-boards-series.html

- Open-source bootloader:
- https://slimbootloader.github.io/supported-hardware/upxtremei11.html

- Build the platform with the updated platform data in the fsp.fd file



Dynamic or Runtime UPD

Bootloader controlled

Configuration Flow with Bootloaders

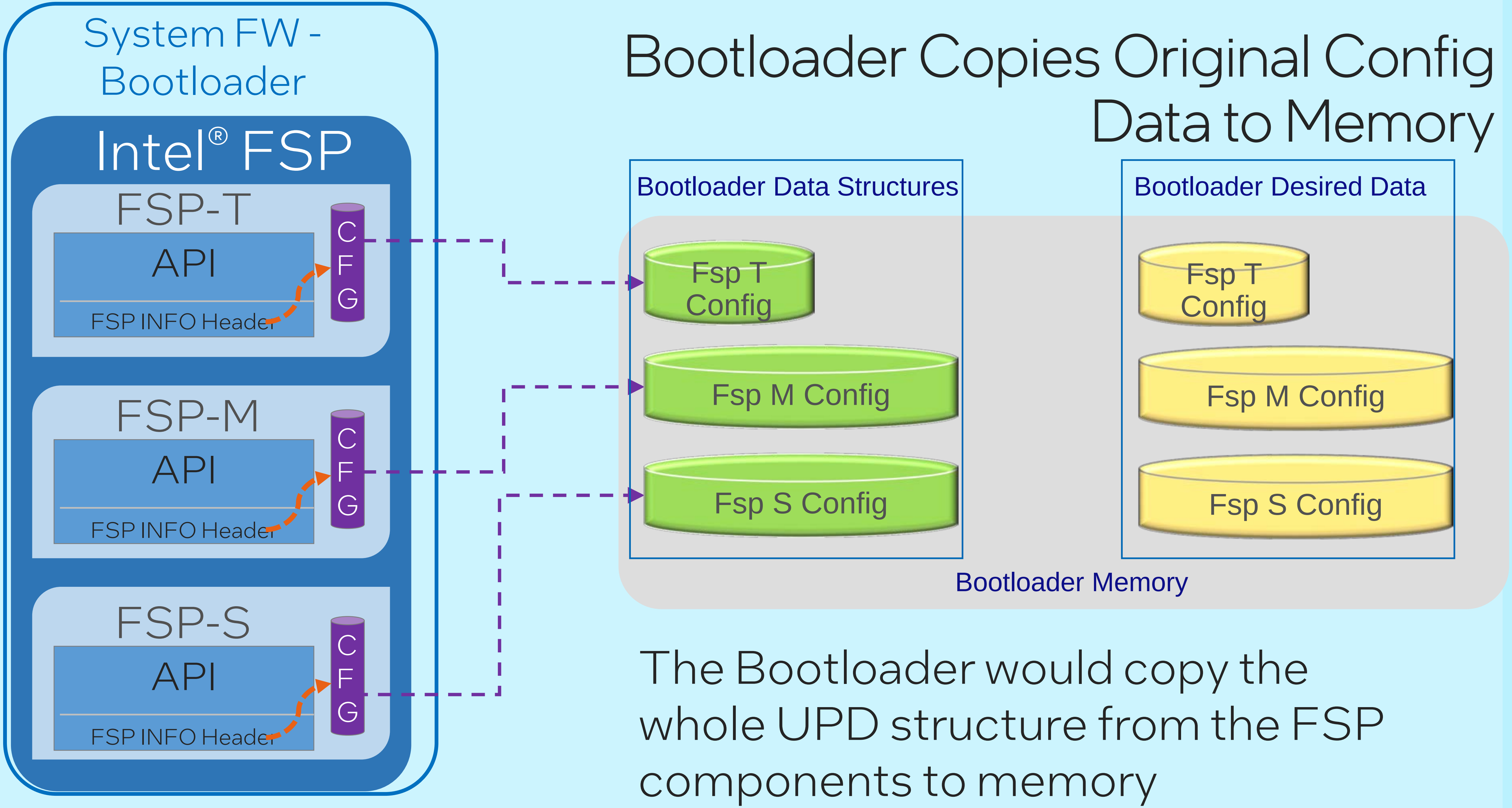
FSP Configuration

- Bootloader build process generates FSP collaterals, such as FD and header files.
- Bootloader engineers consume these collaterals with Static Config Editor tools.

Bootloader Configuration Dynamically Provides Flexibly, But . . .

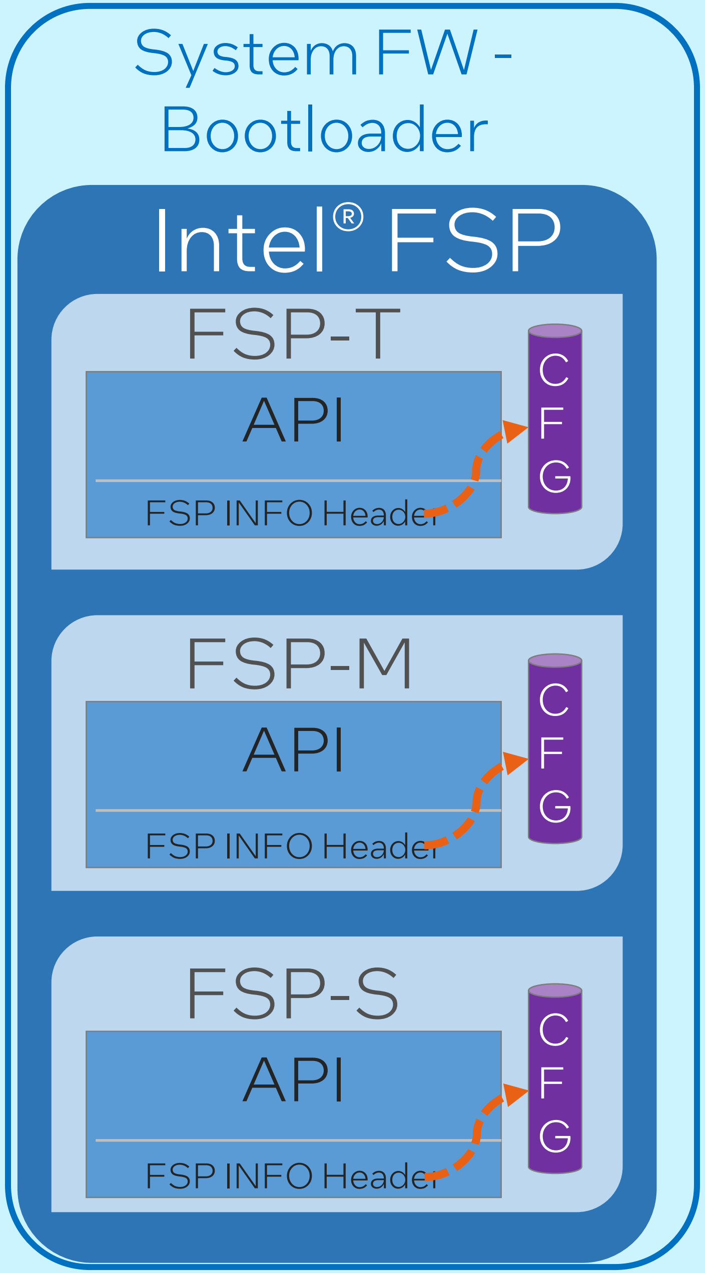
- BIOS Setup
  - Bootloader build process generates HII related files (UNI/HFR/VFR/HPK/I)
  - No UI to render BIOS configurations without booting platform.
- EDK II Platform Configuration Database (PCD)
  - Build time PCDs Versus Setup Dynamic PCDs

Bootloader Copies Original Config Data to Memory



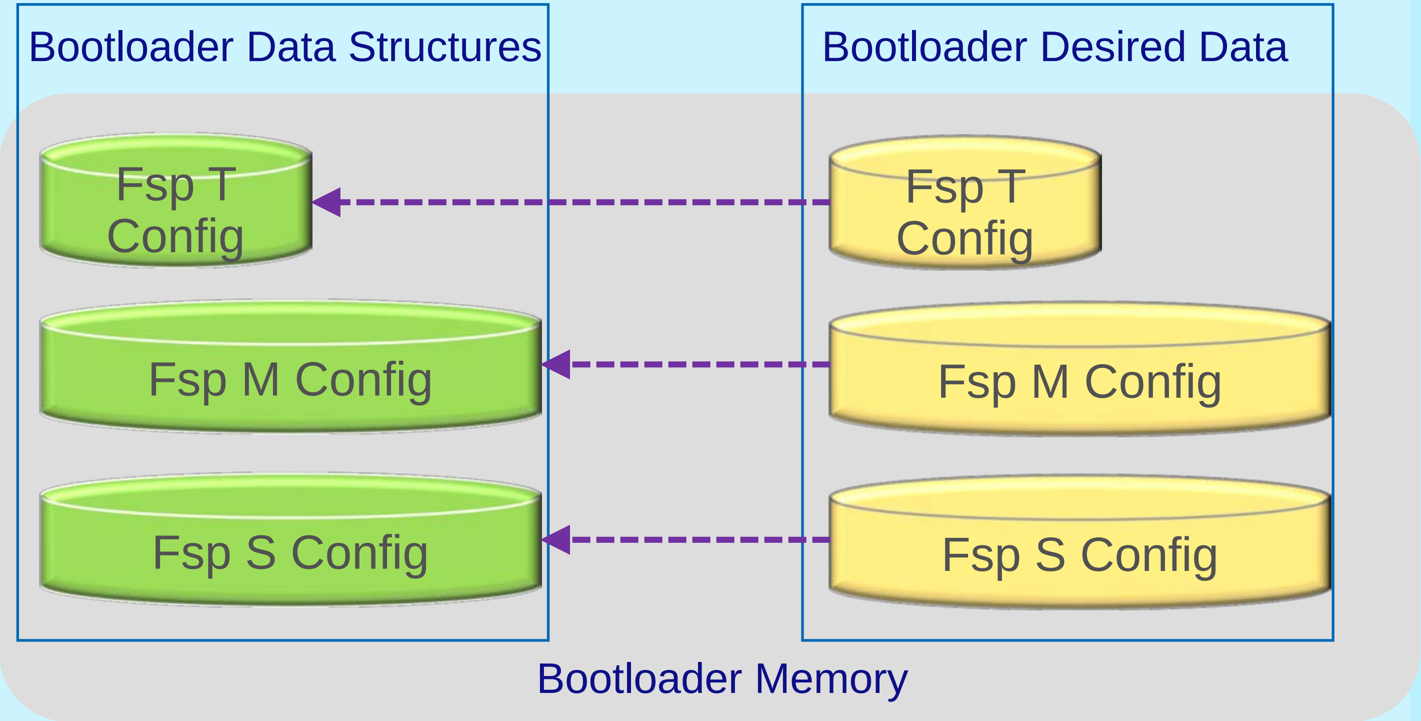
Intel® FSP Spec 2.3 Figure 1

The Bootloader would copy the whole UPD structure from the FSP components to memory



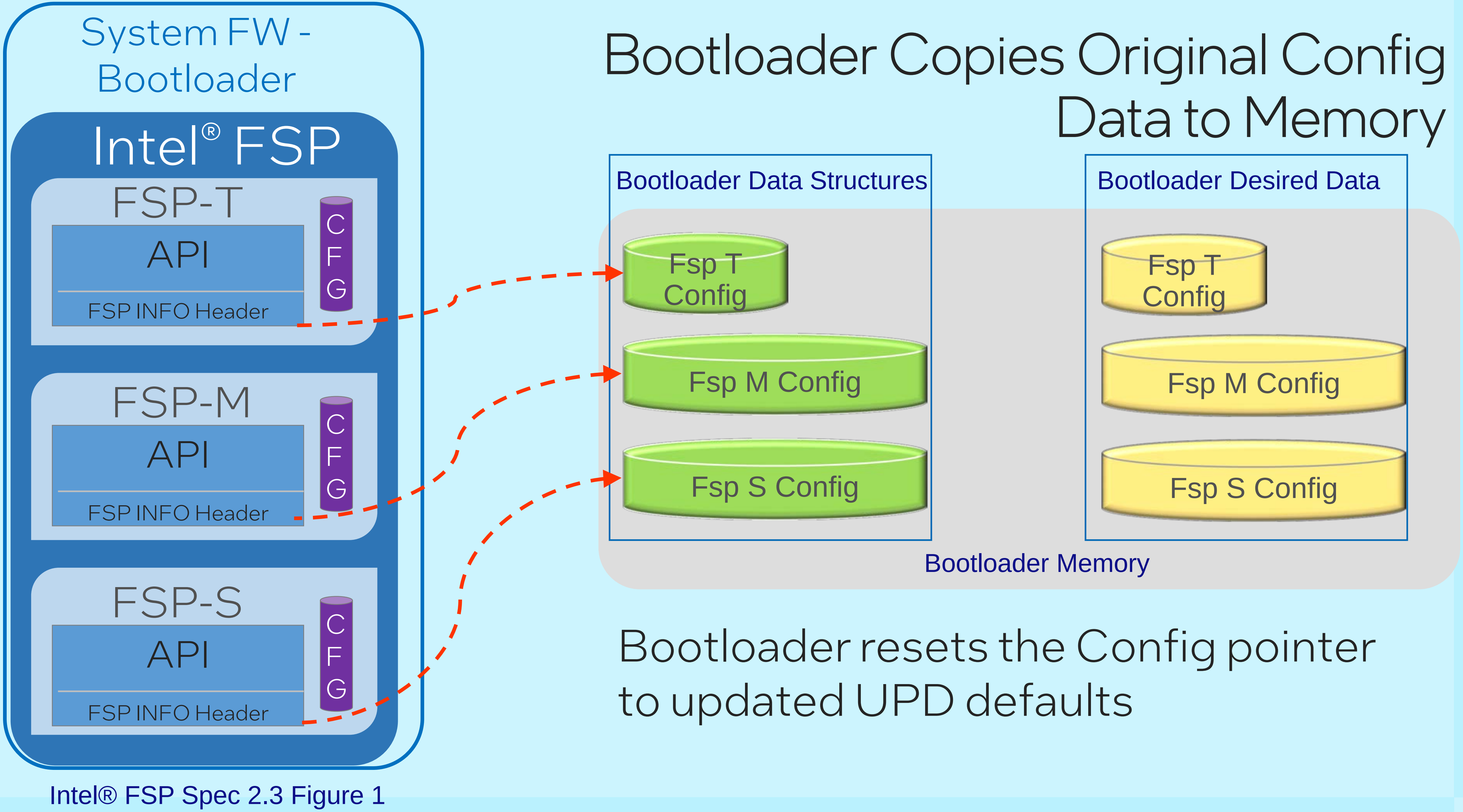
Intel® FSP Spec 2.3 Figure 1

Bootloader Copies Original Config Data to Memory



Bootloader controls the desired data overwriting the original UPD defaults

Bootloader Copies Original Config Data to Memory



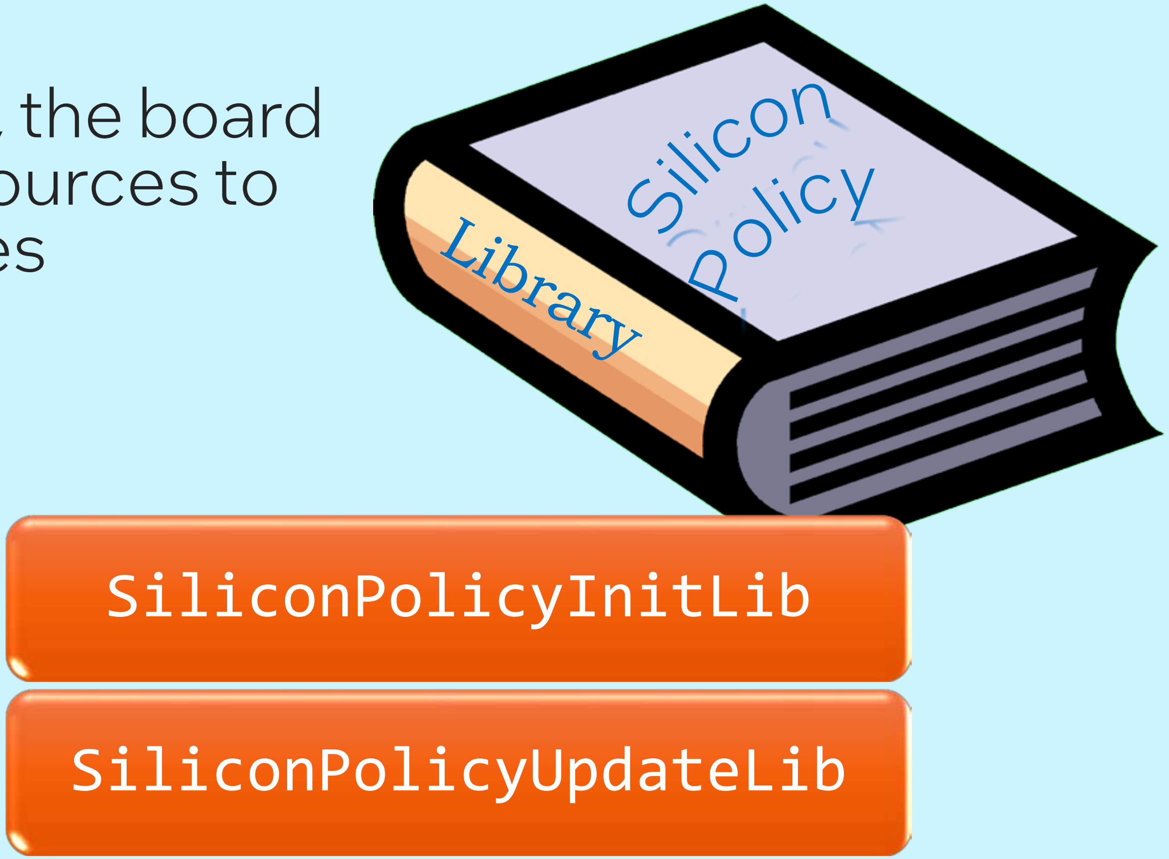
Intel® FSP Spec 2.3 Figure 1

Bootloader resets the Config pointer to updated UPD defaults

Silicon Policy Flow – Minimum Platform Architecture

Using the **SiliconPolicyUpdateLib**, the board package may reference a variety of sources to obtain the board-specific policy values

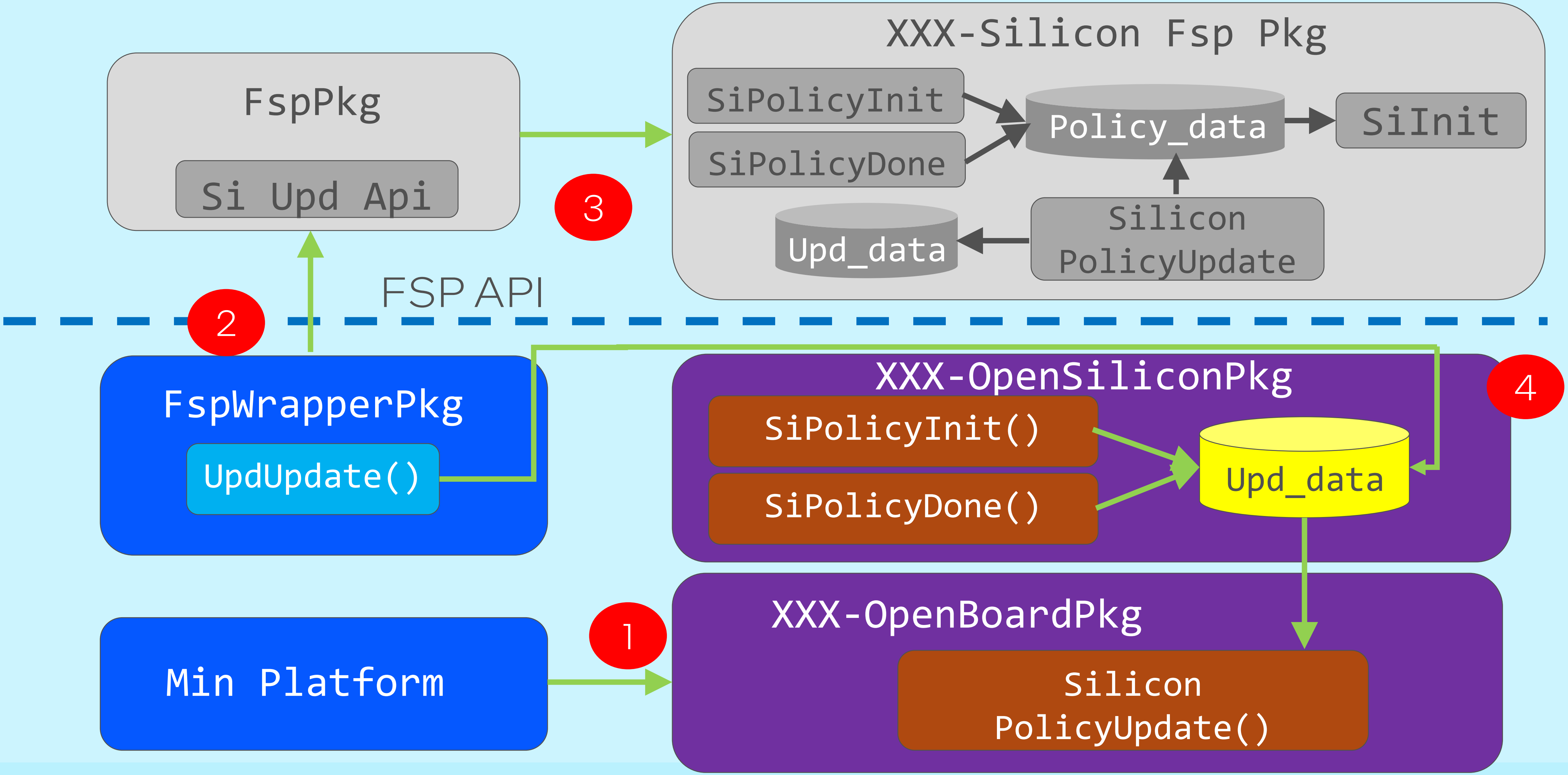
1. PCD database
2. UEFI Variable
3. Binary Blob
4. Built-in C structure
5. Hardware information



One silicon policy data structure created per silicon module

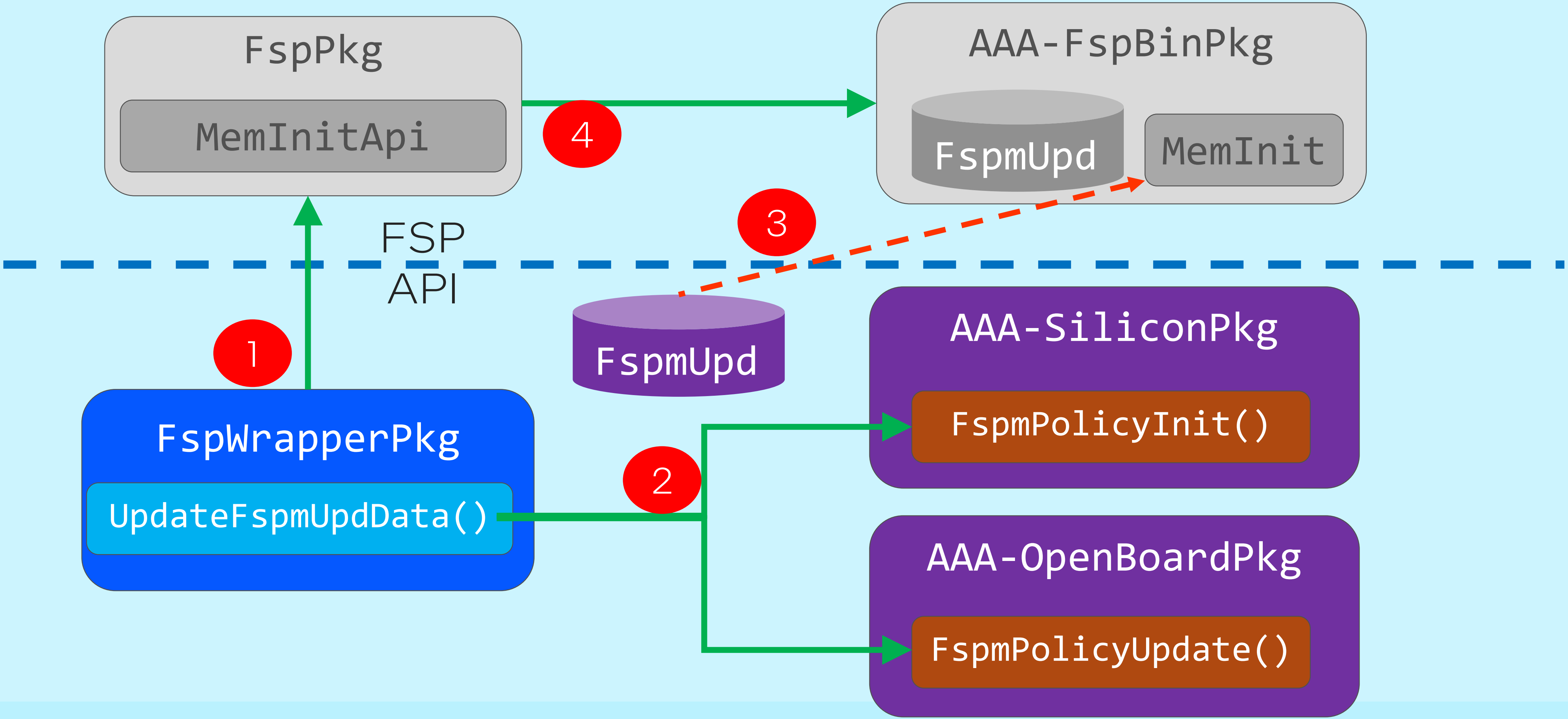
MnimumPlatformSpecification Section 4.6 Data Flows

FSP Silicon Policy Data Flow



MnimumPlatformSpecification Section 4.6 Data Flows

Example: FSP Policy in Platform base on MinPlatformPkg



Update Silicon Policy example

WhiskeyLakeOpenBoardPkg/FspWrapper/Library/PeiSiliconPolicyUpdateLibFsp

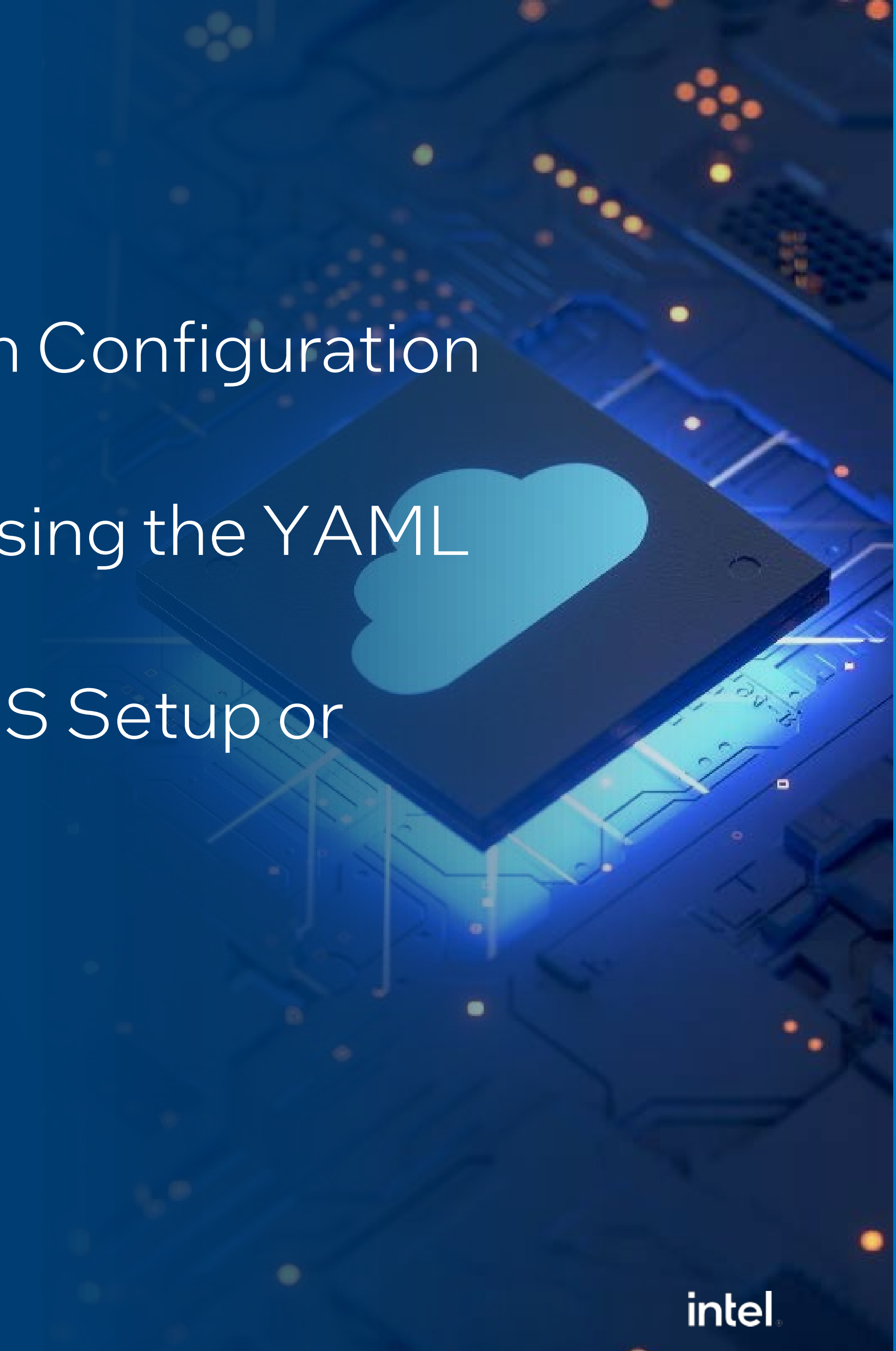
```
EFI_STATUS
EFIAPI
PeiFspSaPolicyUpdatePreMem (
IN OUT FSPM_UPD *FspmUpd
)
{
VOID *Buffer;
// Override MemorySpdPtr
CopyMem((VOID *)(UINTN)\
 FspmUpd->FspmConfig.MemorySpdPtr00,\
 (VOID *)(UINTN)PcdGet32 (PcdMrcSpdData), \
 PcdGet16 (PcdMrcSpdDataSize));
CopyMem((VOID *)(UINTN)\
 FspmUpd->FspmConfig.MemorySpdPtr10,\
 (VOID *)(UINTN)PcdGet32 (PcdMrcSpdData),\
 PcdGet16 (PcdMrcSpdDataSize));
```

```
// Updating Dq Pins Interleaved,Rcomp Resistor &
// Rcomp Target Settings

  Buffer = (VOID *) (UINTN) PcdGet32 \
          (PcdMrcRcompResistor);
  if (Buffer) {
    CopyMem ((VOID *)\
      FspmUpd->FspmConfig.RcompResistor, \
      Buffer, 6);
  } Buffer = (VOID *) (UINTN) PcdGet32 \
          (PcdMrcRcompTarget);
  if (Buffer) {
    CopyMem ((VOID *)\
      FspmUpd->FspmConfig.RcompTarget, \
      Buffer, 10);
  }
  return EFI_SUCCESS;
}
```

Link to file: PeiSaPolicyUpdatePrMem.c

Summary

- It is Important for Customizing the Platform Configuration Per Customer's Needs
- Static Build Time Configuration Updates using the YAML Config Editor
- Dynamic Configuration Updates using BIOS Setup or Other



intel®