presented by

Firmware configuration – Past, Present, and Future

UEFI Fall 2023 Developers Conference & Plugfest

October 9-12, 2023

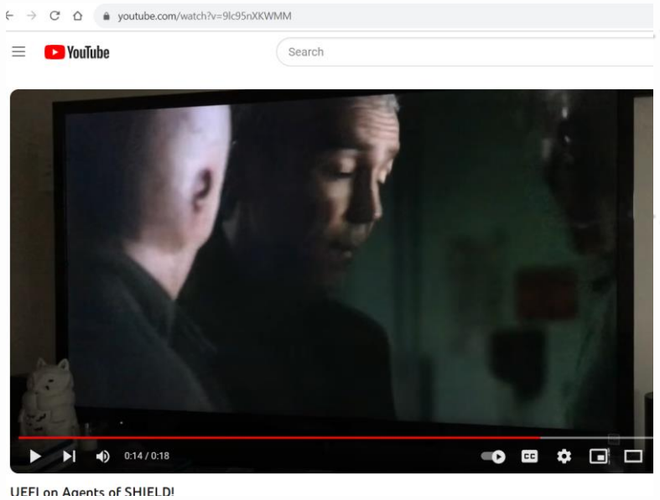
Presented by

Vincent Zimmer (Intel Corporation)

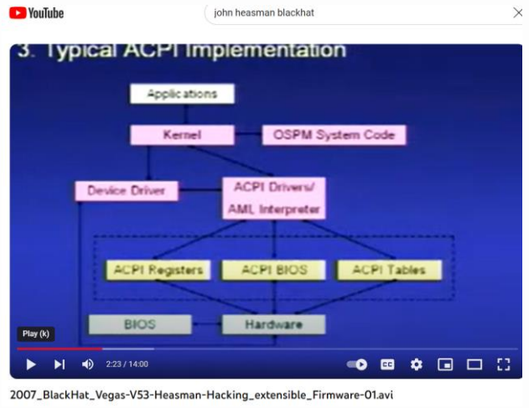
Gahan Saraiya (Intel Corporation)

Christine Chen (Intel Corporation)

Catch up from last 2 days



- U-E-F-I versus YOU-FEE?
- Agent of SHIELD provides not help https://www.youtube.com/watch?v=9lc95nXKWMM (0:8)
- And if YOU-FEE, then ACK-PEE?



  - https://www.youtube.com/watch?v=A0seUVAC09E (1:40)

‘Speaker’ bio’s

Vincent Zimmer

Vincent Zimmer is a Senior Principal Engineer with Intel. He joined Intel in 1997 and has been working on EFI / Framework / UEFI / PI along with touching TCG and other stds groups since 1999. He lives in the Seattle area and can be reached via various paths – *vincent.zimmer@intel.com* *or 425-881-4874* *or* https://twitter.com/vincentzimmer?lang=en or https://www.linkedin.com/in/vzimmer or ….

Gahan Saraiya

Gahan is a skilled Platform Lead at Intel, working within the Software and Advanced Technology Group. With over four years of experience, he has been dedicated to the development and implementation of firmware configurations that support the expansion of automation infrastructure. Gahan's contributions have consistently made a positive and lasting impact on the organization during his tenure.

Know more about Gahan

Christine Chen

Christine is the software development engineer at Intel, has been working on the Edk2 BaseTools related development and support works since 2020. She has designed and developed BaseTools FMMT python tool, and has been participated in BaseTools incremental Build project, BaseTools C tool python convertion work. She is focus on BIOS configuration enhancement in BaseTools build system currently.

Agenda

- Introduction
- Evolution
- Present Practice
- Next Generation of Firmware Configuration
- Questions

Introduction

Introduction

- Growing requirements of various application demands different firmware flows
- Drilled down to classify with conditional flow

Evolution

Evolution

- Boot Flow Control with Firmware Configuration
- HII Implementation

Boot Flow Control with Firmware Configuration

- EFI Variables act as control variable for firmware boot flow process
- Fulfills need of simpler to complex boot flow context, i.e.
  - boot priority ordering
  - security configuration
  - overclocking of device

HII Implementation

HII establishes Infrastructure between external entity to firmware configuration

Control variable (EFI Variable) mapped through various component of HII

vfr/hfr – customized syntactical language to construct user interface

uni – string representation of Identifier mapped in vfr/hfr

Header file *.h – variable structure and GUID

Source file *.c – HII Protocols

Present Practice

Present Practice

- Non-Recommended Practices
- Runtime population of form representation
- Tools and Tech

Present Practice – Non-Recommended Practices

- Action callbacks associated with form representation

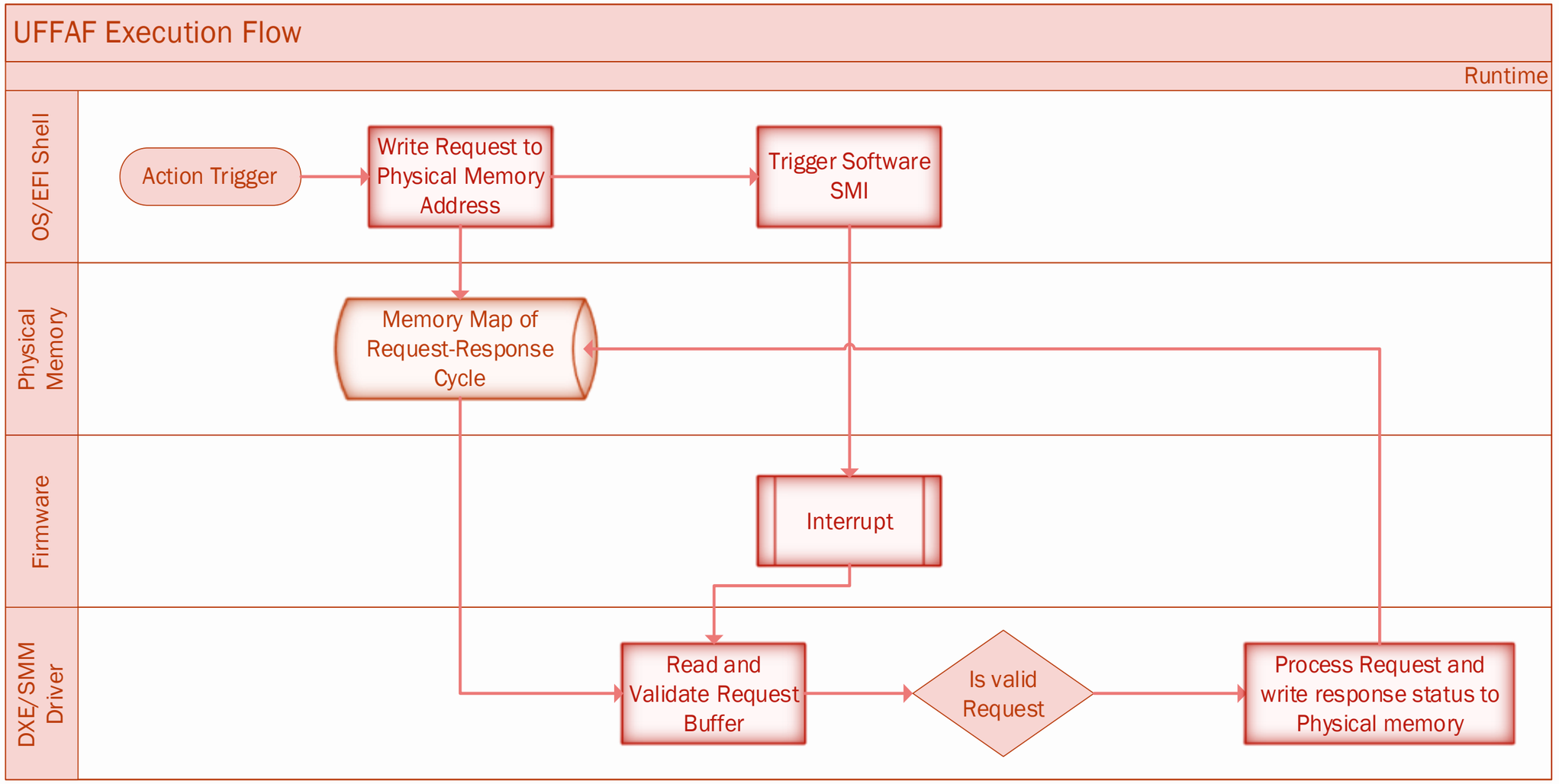
Present Practice - Tools and Tech

TOOL/TECH	REFERENCE
RedFish	DMTF's Redfish®
UFFAF	UEFI Firmware Foundational Automation Framework
USF YAML	yaml boot configuration
FDT	Flattened device tree
FSP UPD	FSP UPD
DFCI	Mu DFCI

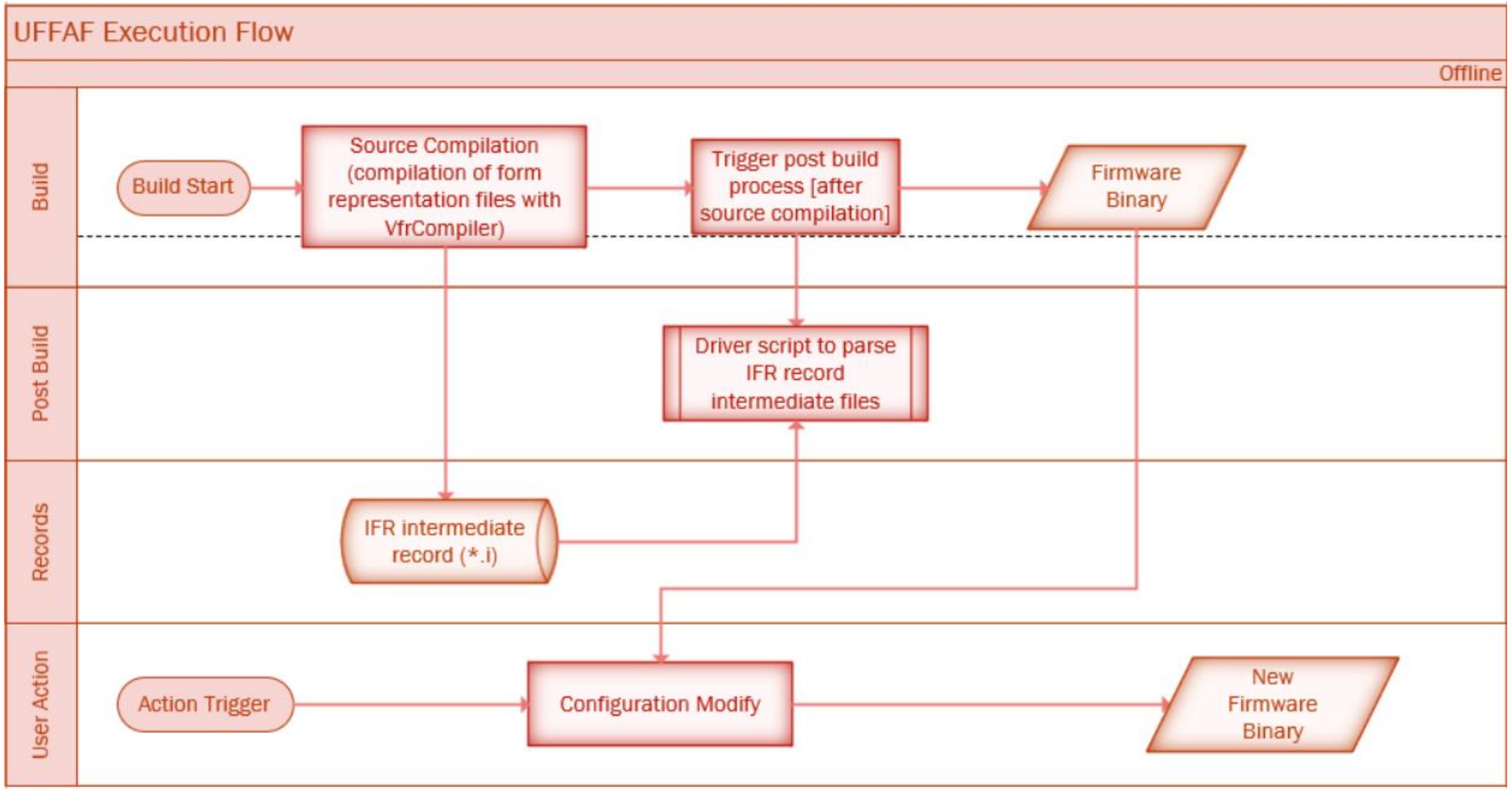
Present Practice - Tools and Tech

Tool	User Visible Data Format	Firmware Implementation	End-User Programming Language
RedFish	json	Edk2 Advanced Feature Package	Python
UFFAF	Xml,json	Intel Advanced Feature Package	Python
USF YAML	yaml	BaseTools	Python
FDT	dts	Device tree compiler (DTC)	C
FSP UPD	Bsf, yaml	Configuration editor	Python

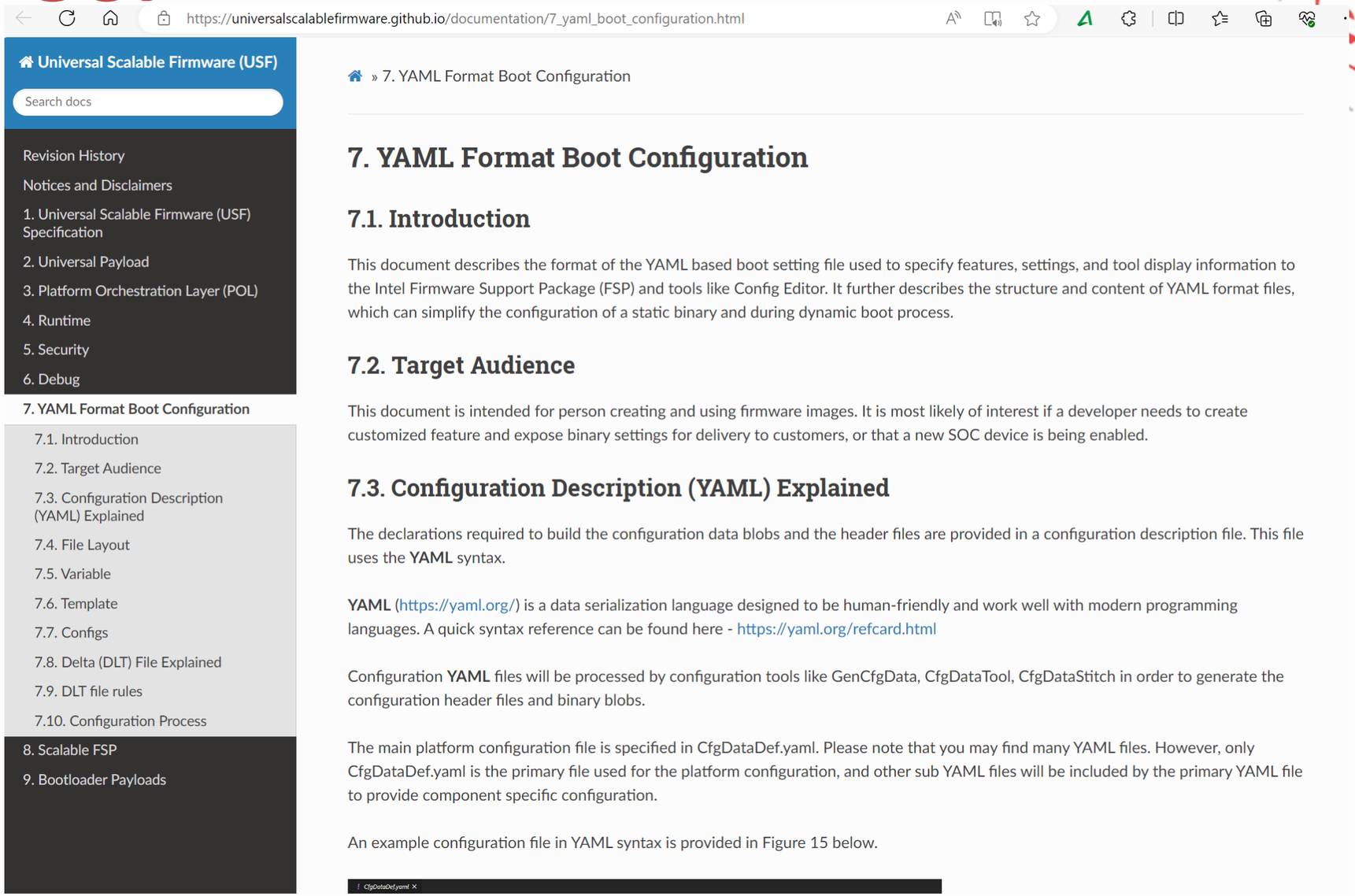
UFFAF UEFI Firmware Foundational Automation Framework



UFFAF UEFI Firmware Foundational Automation Framework

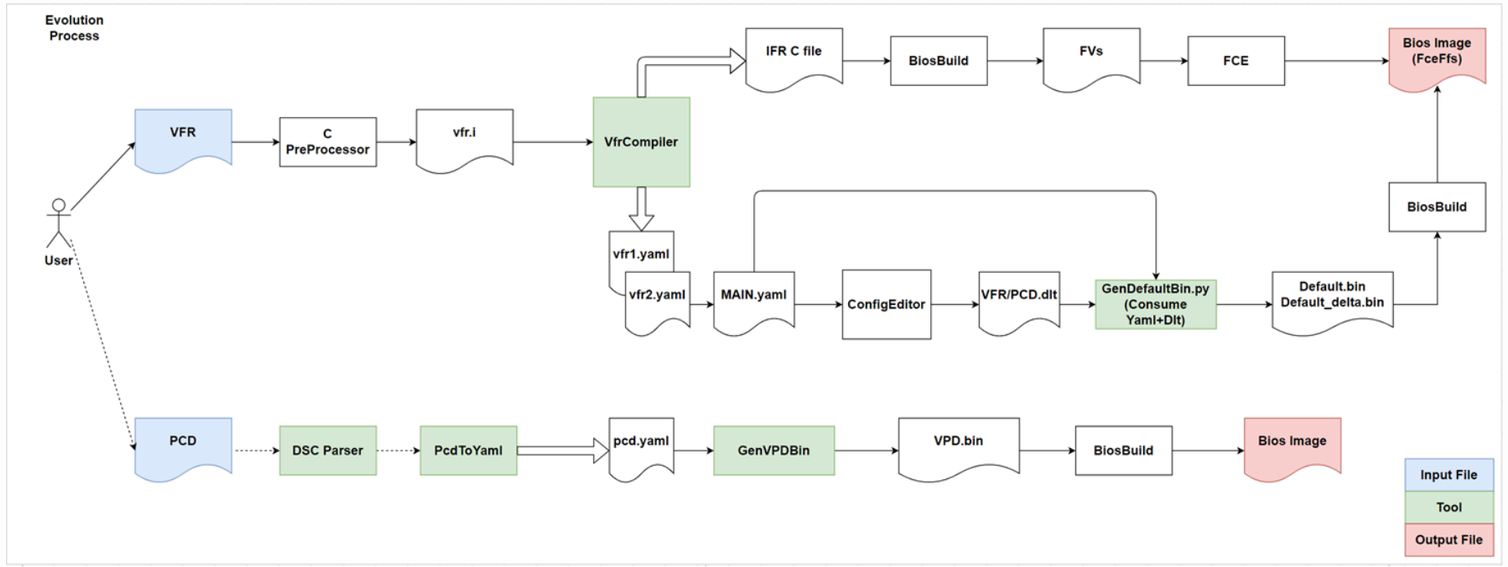


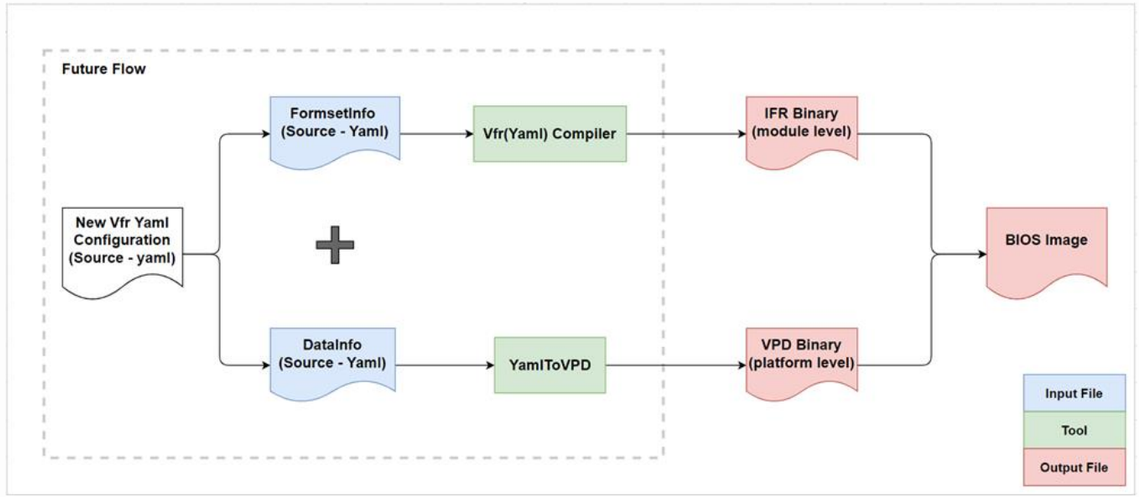
YAML and USF



[7. YAML Format Boot Configuration — Universal Scalable Firmware (USF) documentation]

USF YAML yaml boot configuration



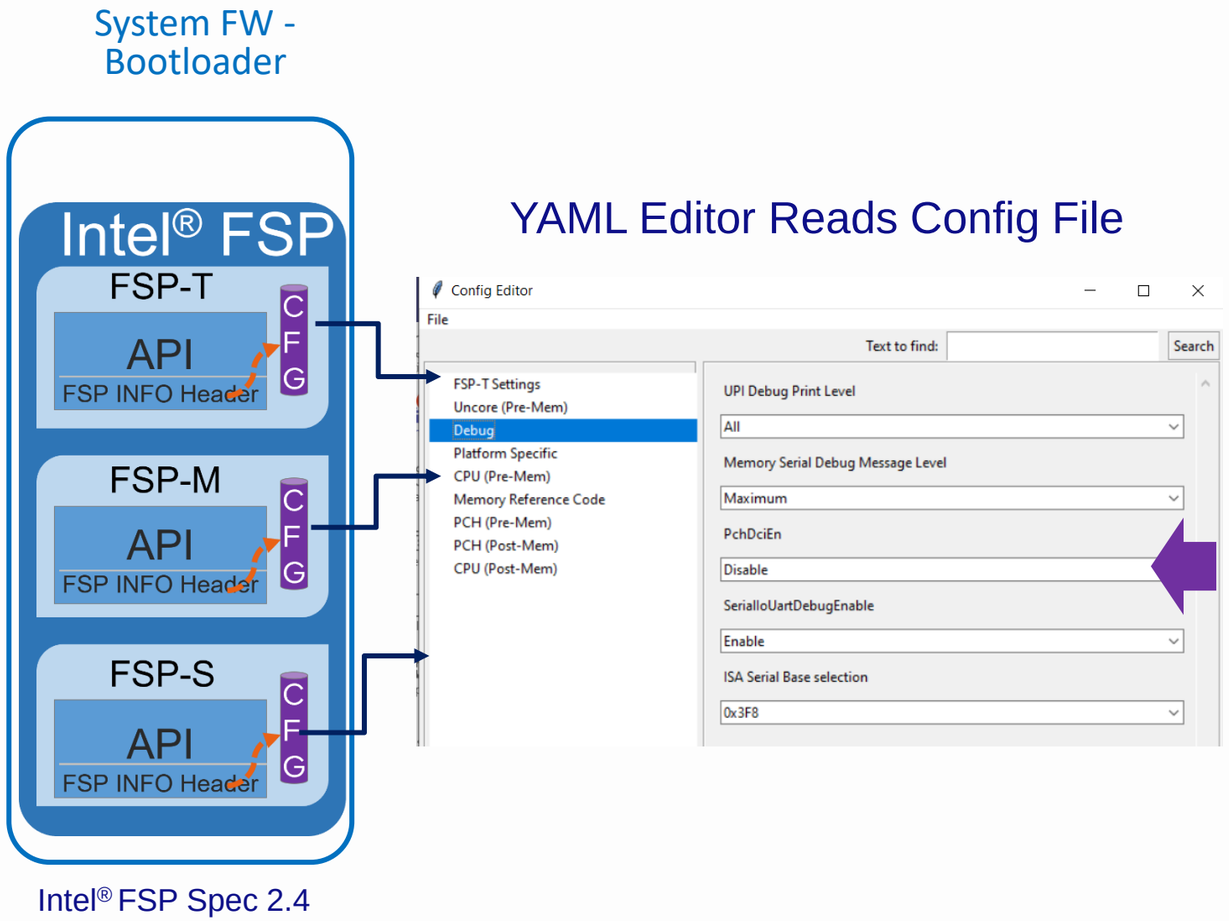


USF YAML focus on the VFR and StructurePCD BIOS Configuration method, expect to unified these source files into YAML type. Based on this expectation, the evolution process in shown as left diagram. For the final flow, all the Bios Configuration related information are from YAML file. YamlCompiler tool and YamlToVPD tool will be used to generate the binary which will be built into the BIOS Image and be consumed during boot time.

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 Boot Setting File (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



Intel® FSP Spec 2.4

https://github.com/tianocore/edk2/blob/master/IntelFsp2Pkg/Tools/UserManuals/ConfigEditorUserManual.md

Next Generation of Firmware Configuration

Next Generation of Firmware Configuration

- Uniting Configuration syntax usage to YAML configuration
- Industry wide standard language syntax with advantageous integration across tech-stack

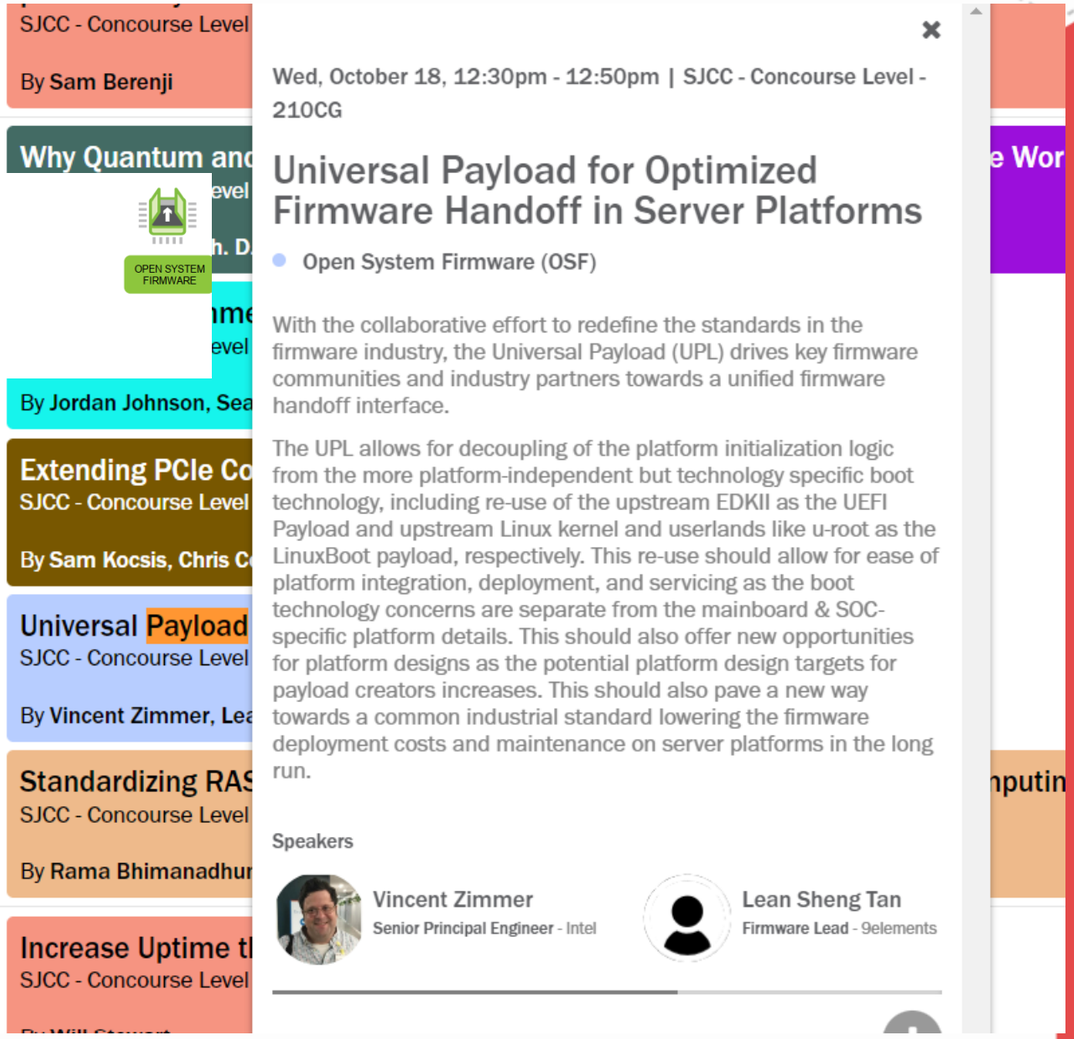
QA

Other events

Flattened devicetree (FDT)

- devicetree.org

See more on FDT at
https://2023ocpglobal.fnvirtual.app/a/schedule/



Thanks for attending the UEFI Fall 2023 Developers Conference & Plugfest

For more information on UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by