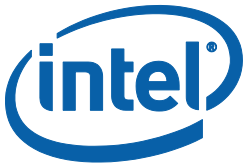


LakeField Platform
Intel® Converged Security Engine (Intel® CSE) Firmware 13.30

Release Notes - NDA

March 2020

Revision 13.30.0.1065 [BKC Release]

Intel Confidential

Read the Important Notes within these Release Notes before flashing a new image.

Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit www.intel.com/design/literature.htm.

Intel and the Intel logo trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Contents

Revision History

Revision Number	Description	Revision Date
13.30.0.7072	• Engineering Release for LakeField	May 2018
13.30.0.7073	• Engineering Release for LakeField	May 2018
13.30.0.7085	• Engineering Release for LakeField	September 2018
13.30.0.7087	• BKC Release for LakeField	October 2018
13.30.0.7093	• Engineering Release for LakeField	November 2018
13.30.0.7095	• BKC Release for LakeField	December 2018
13.30.0.7099	• BKC Release for LakeField	January 2019
13.30.0.1005	• BKC Release for LakeField	January 2019
13.30.0.1005	• BKC Update Release for LakeField	January 2019
13.30.0.1012	• BKC Release for LakeField	February 2019
13.30.0.1012	• Pre-Alpha Release for LakeField	March 2019
13.30.0.1015	• BKC Release for Lakefield	March 2019
13.30.0.1017	• BKC Release for Lakefield	April 2019
13.30.0.1019	• BKC Release for Lakefield	May 2019
13.30.0.1023	• BKC Release for Lakefield	June 2019
13.30.0.1030	• BKC Release for Lakefield	July 2019
13.30.0.1031	• BKC Release for Lakefield	July 2019
13.30.0.1035	• BKC Release for Lakefield	September 2019
13.30.0.1042	• BKC Release for Lakefield	September 2019
13.30.0.1047	• BKC Release for Lakefield	October 2019
13.30.0.1048	• BKC Release for Lakefield	October 2019
13.30.0.1048	• BKC Update Release for Lakefield	November 2019
13.30.0.1048	• BKC Update Release for Lakefield	November 2019
13.30.0.1048	• BKC Update Release for Lakefield	December 2019
13.30.0.1054	• BKC Release for Lakefield	December 2019
13.30.0.1060	• BKC Release for Lakefield	January 2020
13.30.0.1062	• BKC Release for Lakefield	February 2020
13.30.0.1065	• BKC Release for Lakefield	February 2020
13.30.0.1065	• BKC Update release for Lakefield	February 2020
13.30.0.1065	• WW10 BKC release for Lakefield	February 2020

1 Introduction

1.1 Scope of Document

This document provides component level details of the downloaded kit and the contents of each folder in the kit.

1.2 Acronyms

Term	Description
BIOS	Basic Input Output System
CIM	Common Information Model
Dekel PHY	Dekel firmware supports functionality of PHY controllers like UFS, PCIe and 2 Type-C USB ports.
FW	Firmware
GbE	Gigabit Ethernet
HBC	Host Based Configuration
HECI	Host Embedded Controller Interface. Same as Intel® MEI.
CRB	Customer Reference Board
Intel® DAL	Intel® Dynamic Application Loader (Intel® DAL)
Intel® FIT	Intel® Flash Image Tool
Intel® ICCS	Intel® Integrated Clock Controller Service
Intel® MEI	Intel® Converged Security Engine Interface (Interface between the Management Engine and the Host system).
Intel® PETS	Intel® Platform Enablement Test Suite
Intel® PTT	Intel® Platform Trust Technology
ISV	Independent Software Vendor
IUP	Independently Updatable Partitions
MRC	Memory Reference Code
OS	Operating System
PCH	Platform Control Hub
PFT	Platform Flash Tool. This tool supports DnX use case / functionality over USB.
PMC	Power Management Controller
SPI	Serial Peripheral Interface
SUT	System Under Test
SVN	Security Version Number. Used in Firmware Upgrade / Downgrade capabilities.

Term	Description
UFS	A Type of non-serial flash block media devices.
VCN	Version Control Number. Used in Firmware Upgrade / Downgrade capabilities.

2 Release Kit Summary

This document covers the following Intel® Converged Security Engine Firmware SKUs for the LakeField Series platform:

2.1 Release Kit Details

Firmware Support	This Firmware supports boot from SPI and UFS. There are separate firmware binaries included in the kit targeted for SPI and UFS boot Media usage. Based on boot media targeted to be used, customers are recommended to integrate respective firmware binary to create IFWI image. Features Supported: Load and Authentication of FWs like PMC FW, Dekel PHY FW and ISH FW. Intel® ICCS, Intel® Platform Protection Technology with Boot Guard, PAVP, DnX, RPMB, PTT, Power Flows.
Kit Release	Build Number – 13.30.0.1065
Target Platform	LakeField Series Platform

2.2 Kit Overview

The kit can be downloaded from Intel® VIP (https://platformsw.intel.com/).

Note: A username and password are required to access the website and to log in. User must have an account created for access.

1. After logging in, click on the link 'View All Kits' on the left side of the web page.
2. Click on the corresponding kit number that is to be downloaded.
3. Select and open the appropriate kit component.
4. The Supporting Documentation folder under the selected component contains the following supporting documentation:
    a. FW Release Notes – This document gives an overview of the contents of the entire downloaded component. Also provides the details on closed and open Sightings and bugs with this kit release.
    b. BIOS Release Notes – This document provides details of BIOS issues resolved with the kit.
5. Click on the Installation Files folder under the selected component and extract the .zip kit into a folder (Example: C:\).

2.3 Contents of Downloaded Kit

Download the kit, as previously specified, into the directory (C:\). The details of the contents and directory structure are listed below:

2.3.1 SW Components

Installers	Description
ME_SW_DCH	This folder includes the DCH compliant drivers.
Intel® MEI Driver	• Intel® MEI is the interface between the host and the Intel® Converged Security Engine. • Drivers and applications on the host that wish to interact with Intel® Converged Security Engine through the host interface use the Intel® MEI host Windows* driver.
iCLS Driver	• iCLS Client is a set of applications, services and dynamic libraries used to establish a trusted connection between FW and Intel's backend. **NOTE:** iCLS driver is not available in the kit release.
JHI Driver	• This driver is capable of loading and executing code (DAL Application) in a build-in isolated VM environment. • This driver is capable of utilizing Intel® CSME capabilities.
Intel® SPD	This driver enables the Intel® Trusted Execution Engine Storage Proxy Device.

2.3.2 Image Components

Image	Description
Intel® CSE	• The Intel® Converged Security Engine firmware contains code and configuration data for Intel® Converged Security Engine functions. • This is one of the regions that are integrated into the final flash image that is built using the Flash Image Tool, and is then programmed into the flash. • There are two firmware binaries included in the kit one for SPI and one for UFS. **NOTES:** 1. For more details on building the flash image, refer to **FW Bringup Guide** included in the downloaded kit. 2. For more details on the firmware and related issues, refer to **Important Notes** section of this document.
DnX	• DnX_Module - A binary file signed by Intel. This file has the DnX logic ME ROM to run and included in the Intel® CSE kit for Lake field Platform. • DnX is Intel's proprietary solution to download Integrated Flash Image (IFWI) to a target machine from a host machine by means of USB cable. Intel® DnX flows are executed over fixed USB 2 port.

Image	Description
PMC	• The PMC firmware contains code for power management controller functions. • This is one of the regions that is integrated into the final flash image that is built using the Intel® FIT tool, and is then programmed into the SPI flash. **NOTE:** For more details on the PMC related issues, refer to **PMC changes** section of this document.
Dekel PHY	Dekel PHY – A binary signed by Intel. This file binary is responsible for handling the configuration and functionality PHY Controller for UFS, PCIe and Type-C USB ports. **NOTE:** For more details on the Dekel PHY FW related issues, refer to Dekel PHY changes section of this document.
PCHC	PCHC – A binary signed by Intel. This file binary is responsible for handling the configuration of PCH clock parameters. **NOTE:** For more details on the PCHC FW related issues, refer to PCHC changes section of this document.

2.3.3 System Tools

Refer to the **System Tools User Guide** for details on tool usage.

Tool	Description
Intel® Flash Image Tool	• Used to assemble the different elements of the SPI flash Descriptor, Intel Reference System BIOS, Intel® Converged Security Engine, PMC and Dekel PHY into a single binary image. • Provided as a GUI tool. • **OS Support:** — Refer to LakeField PRD.
Intel® Flash Programming Tool	• Used to write the flash image into the SPI flash device. • DOS*, EFI* and Windows* command line tools provided. • **OS Support:** — Refer to LakeField PRD.
FWUpdate	• Used to update the Intel® Converged Security and Management's firmware. • DOS*, EFI* and Windows* command line tools provided. • Reduced Sized Intel® FWUpdate API Library is available under Tools/System_Tools/FWUpdate_RS. • **OS Support:** — Refer to LakeField PRD. **Note:** This is not included in the FW kit.

Tool	Description
MEInfo	• Verifies that Intel® Converged Security Engine (Intel® CSE) firmware is alive and returns data about Intel® CSE. • DOS*, EFI* and Windows* command line tools provided. • **OS Support:** — Refer to LakeField PRD. **Note:** The MEInfo tool is specific to the boot media type.
MEManuf	• Used on the manufacturing line to validate platform is configured properly. • DOS*, EFI* and Windows* command line tools provided. • **OS Support:** — Refer Tools PRD.
Intel® MEU	• Signing and Manifesting tool. • For usage instructions refer to the **Signing and Manifesting Guide** included in the downloaded kit.

2.3.4 DnX Tool

Tool	Description
Intel® Platform Flash Tool (Intel® PFT)	Intel implementation of DnX and secure token flows. This tool runs on remote host computer. DnX module and IFWI.bin are inserted to the target machine via this tool and included in the Intel® CSE Kit for LakeField platform.

2.4 Release Version Numbering Information

Typical release version numbering is as follows,

13.30.y.z (for example: 13.30.0.zzzz) where:

'13' refers to the Intel® Converged Security Engine 13.0 Firmware for LakeField Platform.

'0' represents the associated platform program.

[0-9] – Client platform programs
[10-19] - *Falls Workstations and HEDT
[20-29] - *leys Workstations
[30] - LakeField
[40-99] – Reserved for future program needs

'y' refers to Maintenance and Hot Fix release designations.

'z' refers to firmware release revision.

2.5 Firmware Update Information

Intel® CSE Firmware Update (either upgrade or downgrade) is evaluated based on the ARB SVN value, the VCN value, or the PV values. These values work in unison and can impose restrictions at the same time.

2.5.1 Firmware Update Terminology

ARB SVN (Anti-Rollback Security Version Number) is used to prevent downgrade the current firmware to a firmware with a lower ARB SVN number.

If Hardware ARB SVN committed (FPF fuses burned), systems will not be able to downgrade to a firmware with a lower ARB SVN number even when physical access to the platform is possible.

TCB SVN (Trust Computing Base Security Version Number): The Intel® CSE generates multiple keys that are part of the TCB of Intel® CSME. When critical vulnerabilities are found that compromise the TCB the TCB SVN is subsequently increased and "TCB Recovery" is triggered.

The TCB Recovery revokes the compromised credentials and replaces them with new ones.

VCN (Version Control Number): will be incremented if there is a security fix, a significant firmware change or a new feature addition. A downgrade to lower VCN value will be prohibited.

PV (Production Version): Intel® CSME Firmware will have a PV bit set. Upgrade to a non-PV firmware is not allowed. An update from non-PV version to a PV is allowed.

Update rules:

- If the system is at PV (Production Version) quality firmware that has PV bit set, update to non-PV firmware is not allowed. Only Non-PV to PV is allowed.

- Example: 12.0.0.zzzz PV cannot upgrade to 13.0.0.zzzz Alpha
- Update to firmware that has lower ARB SVN (Anti-Rollback Security Version Number) is not allowed.
- Update to firmware that has lower VCN (Version control number) is not allowed.
- Update across major point release is not allowed for example 10.x to 11.x.
- If firmware update setting in Intel® MEBX is password protected, Intel® MEBX password must be supplied during the update.

2.5.2 VCN Firmware Upgrade or Downgrade Table

Intel® CSE FW Version	ARB SVN #	TCB SVN #	VCN #	PV (1 or 0)
13.30.0.7072 (ENG Release)	1		0	0
13.30.0.7073 (ENG Release)	1		0	0
13.30.0.7085 (ENG Release)	1		0	0
13.30.0.7087 (BKC Release)	1		0	0
13.30.0.7093 (BKC Release)	1		0	0
13.30.0.7095 (BKC Release)	1		0	0
13.30.0.7099 (BKC Release)	1		0	0
13.30.0.1005 (BKC Release)	1		0	0
13.30.0.1012 (BKC Release)	1		0	0
13.30.0.1012 (Pre-Alpha Release)	1		0	0
13.30.0.1015 (BKC Release)	1	1	1	0
13.30.0.1017 (BKC Release)	1	1	1	0
13.30.0.1019 (BKC Release)	1	1	1	0
13.30.0.1023 (BKC Release)	1	1	1	0
13.30.0.1030 (BKC Release)	1	1	1	0
13.30.0.1031 (BKC Release)	1	1	1	0
13.30.0.1035 (BKC Release)	1	1	1	0
13.30.0.1042 (BKC Release)	1	1	1	0

Intel® CSE FW Version	ARB SVN #	TCB SVN #	VCN #	PV (1 or 0)
13.30.0.1047 (BKC Release)	1	1	1	0
13.30.0.1048 (BKC Release)	1	1	1	0
13.30.0.1054 (BKC Release)	1	1	1	0
13.30.0.1060 (BKC Release)	1	1	1	0
13.30.0.1062 (BKC Release)	1	1	1	0
13.30.0.1065 (BKC Release)	1	1	1	0

3 General Information

3.1 Important Notes

- CSE introduced performance improvement in DnX module - improve UFS flash time from ~60sec to ~8sec. Improvement affects configpart command when UFS device Ref. Clock is not 19.2MHz, UFS 3.0 devices come with 26.0MHz as default while Intel supports UFS default frequency High speed in 19.2MHz only, In such case, namely a 26.0MHz device, CSE is required to configure device to 19.2MHz in PWM mode only, That can't be done according above performance improvement implementation. Fix introduced preserve preserves the performance optimization and was further improved to ~7sec.
- A new lite version of the Intel® Platform Flash Tool (Intel® PFT) will be included.
- The Window* base versions of the FPT tool executable have been reduced in size.
- The PCHC binaries are specific to the stepping of LakeField being used.
- PM flows currently blocked on SPI and UFS currently under investigation.
- This kit includes the DCH compliant installer for drivers and is supported on Win 10 RS3 and above versions.
- Workaround in this release for Delayed Authentication Mode enable need global reset instead of cold reset from BIOS.

  SPI – Fixed USB Type-C functionality after G3 working with DAM on SPI.

  UFS – Still requires debug with BIOS.

3.2 Hardware Configurations

This release supports the following HW configurations:

- LKF B-Step (ES)

3.3 Best Known Configuration

For the latest Client Based LakeField Series Platforms Best Known Configuration (BKC), contact platform CE.

4 Kit Details

4.1 Build Details

Component	Version#	Changes Since Previous Release
Intel® CSE Firmware	13.30.0.1065	No
PMC	133.0.10.1037	Yes
PCHC Version	13.30.0.1005 B-Step	No
Dekel PHY	10.218.203.1136 B-Step	Yes
SW Installer Version	2005.13.30.9091	No
Intel® MEI Driver Version	1950.13.30.9079	No
JHI	1.34.2019.0714	No
SPD	1950.13.30.9079	No
iCLS	1.55.66.0 Submission ID: 1152921504627996765 Shared Product ID: 1152921504607682290	No
Tools	13.30.0.1065	No
PFT	5.9.5.0	No

4.2 Intel® FIT XML Changes

4.2.1 Intel® FIT XML Change Log

Changes	Firmware Version
• Ports D and F removed from HDCP Internal Display Ports 1 and 2 drop downs.	13.30.0.7073
• Permissions updated to include extended regions. • System Integrator ID settings removed. • RPMC settings removed. • BCLK SSC Max settings default changed to 0.50. • Removed ITPXDP, LPC0 and LPC1 settings from Clock Output Configuration. • XHCI Port settings added.	13.30.0.7085
• Target Type setting removed. • APWROK Enabled setting removed. • Persistent PRTC Backup Power setting default changed to 'None'. • Debug Override Pre-Production Silicon setting default changed to '0x300017'.	13.30.0.7087
• PCH Configuration Sub-Partition added. • Persistent PRTC Backup Power default changed to 'None'. • UFS Configuration section added.	13.30.0.7093
• FPF Anti-Rollback settings added. • Pre-Production Debug Override value updated. • Type-C Sub System section and Dekel PHY designation changed.	13.30.0.7095
• IPU Debugging removed. • DnX binary output path updated.	13.30.0.7099
• DnX binary path changed. • Redundant FIT option for DekelAuthenticateEn removed.	13.30.0.1005
• MobileSigningUtil removed from Signing Tool setting. • End of Manufacturing Enable setting added. • 24Mhz Crystal Shutdown Wait Interval removed.	13.30.0.1012
• PMC Length value updated • PMC Max Length value updated • Quad IO Read Enable default changed to "Yes" • Quad Read Enable default changed to "Yes" • OPI Link Speed default changed to 4GT/s • I2C speed settings changed to Standard, Fast and Fast Plus. • Platform IMON changed from hex entry type to Enabled/Disabled drop down.	13.30.0.1015
• Top Swap Block Size help text updated. • BIOS Guard help text updated. • Debug Override Pre-Production Silicon value changed.	13.30.0.1017
• No Change	13.30.0.1019
• SPI clock frequencies updated • ICC BCLK values updated • DnX settings updated	13.30.0.1023
• No Change	13.30.0.1023
• PCIe Lane configuration settings removed from FIT UI	13.30.0.1030

Changes	Firmware Version
• Intel(R) Trace Hub Soft Enable removed from FIT UI	
• XML Label updates ISH Input File and ISH PDT • Help text for DnX	13.30.0.1031
• Default for MMP UFSX2 and UFSX2 settings changed to Yes.	13.30.0.1035
• FPF Anti-Rollback settings removed	13.30.0.1042
• Added NFTP/FPTR settings • Spacing correction for eSPI / EC Slave 1 Device Maximum I/O Mode for drop down settings • PMC_Strap_pmc_smip_PLL_BASED_XTAL_DISABLE_Diff value added	13.30.0.1047
• I2C Communication Speed default changed to Fast Plus • PMC_Strap_pmc_smip_CPWRG_STCH_WTDIS_Diff value changed to 0x0	13.30.0.1048
• No Change	13.30.0.1048
• RPMC Configuration settings added • Intel® Trace Hub Filtering setting added • Hyperthreading enabled by default • Values changed for: PCH_Strap_fproxy2_DMI_TLPFTM_Diff PCH_Strap_fproxy2_spare_softstrap_Diff PCH_Strap_PCIE1_RPCFG_Diff PCH_Strap_PCIE0_P1PNCCWSSCMES_Diff PCH_Strap_PCIE0_RPCFG_Diff PCH_Strap_ISH_ISH_Core_Sel_Override_Val_softstrap_Diff PMC_Strap_pmc_smip_LAN_PHY_PU_TIME_Diff PMC_Strap_pmc_smip_GP29MGPIO3_SLPWLAN_SEL_Diff PMC_Strap_pmc_smip_CNVI_1P8_LDO_EN_Diff PMC_Strap_pmc_smip_CPWRG_RST_WTDIS_Diff PMC_Strap_pmc_smip_MPHY0_DIS_STRAP_Diff PMC_Strap_pmc_smip_MPHY1_DIS_STRAP_Diff PMC_Strap_pmc_smip_MPHY2_DIS_STRAP_Diff PMC_Strap_pmc_smip_MPHY3_DIS_STRAP_Diff PMC_Strap_pmc_smip_GPIOCOM5_DIS_STRAP_Diff PMC_Strap_pmc_smip_GPIOCOM4_DIS_STRAP_Diff PMC_Strap_pmc_smip_PLL_BASED_XTAL_DISABLE_Diff PMC_Strap_pmc_smip_BMSDRP_Diff	13.30.0.1054
• Removed Processor Emulation • I2C default changed from Fast Plus to Fast • Removed PMC_Strap_pmc_smip_CPWRG_RST_WTDIS_Diff	13.30.0.1060
• Processor Boot Max Frequency setting changed to No	13.30.0.1062
• No Change	13.30.0.1065

4.2.2 Intel® FIT XML Compare / Delta from Previous Release

Intel® CSE 13.30.0.1062 Release	Intel® CSE 13.30.0.1065 Release

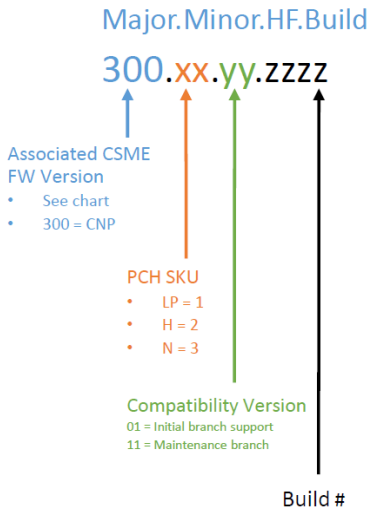
4.3 PMC Changes

PMC FW –Release Version Numbering Information

- PMC FW is PCH SKU (H vs. LP) as well as PCH stepping dependent.
- **Major = Associated Intel® CSME FW Version**

  For CNL (legacy naming), follows Chipset Family Series '300'

  For ICL, LKF and moving forward, follows Intel® CSME FW Version:



(Examples)

Platform	CSME FW Version	PMC Version
CNL / CFL (ME12.0)	12.0.00.zzzz	300.2.01.1001
ICL (ME13.0)	13.0.00.zzzz	1300.1.01.1001
LKF (ME13.30)	13.30.00.zzzz	1330.0.01.1001

- **Minor = PCH SKU (Example: H vs LP vs SoC)**

  'x' refers to the Intel® PCH Type SKU PMC FW is supported for 0 = SoC (i.e. LKF), 1 = LP, 2 = H

- **HF = CVN# -Compatibility/Maintenance Version number**

  Aligned with PMC Engineering branch.

  'yy' refers to the Compatibility/Maintenance build. This field indicates when PMC FW is updated to comply with new requirements; i.e.: HW support or features.

  - 01 = Initial branch support
  - 11 = Maintenance branch with new stepping support

- **Build# -Release version**

Use 4 digit # mechanism to align it with ME FW build#

Start build # with 1xx1 for official release

Increment last digit to indicate patch's compatibility with HW stepping; if new stepping comes up which needs new patch, re-start it with 1xx1.

For any Eng. release, start build# with 7xxx to differentiate between official vs. debug/Eng. drop.

4.3.1 PMC Important Notes

4.3.2 PMC Change Log

PMC Version	Changes	Firmware Version	Stepping Supported
LKF_A0_PMC_FW_PATCH_V2	PMC updated for CPU Bridge SID and DID programming.	13.30.0.7072	A
LKF_A0_PMC_FW_PATCH_V3	Changes to support CrashLog dump. VCCIO rail address change in PMC from SMPS 9 to SMPS 6. Requirements for powergating are added. Fix for Host reset issue caused by SUSPMCFG register bit.	13.30.0.7073	A
LKF_A0_PMC_FW_PATCH_V4	Support for ICC wake signal assert for Soi3 added. Changes added for CrashLog completion status. Changes added to support S0ix Entry. Removed Soix wake timer support as it is not applicable to LKF.	13.30.0.7085	A
LKF_A1_PMC_FW_133.0.01.1005	System performs cold reset without going into global reset on resume. Power stable signal being deasserted after warm reset as expected. During Global Reset the Power management assert signal shows valid levels for sufficient time when global reset is triggered.	13.30.0.7087	A
LKF_A1_PMC_FW_133.0.01.1009	During reset entry (warm and other similar resets), while Boot from UFS feature is enabled, MMP vnn_aon_reset is de- asserted as soon as BM IPs are out of reset.	13.30.0.7093	A
LKF_A1_PMC_FW_133.0.01.1011	I^2C speeds adjusted at values which allows for no failure rates with I^2C transactions. PMC FW to send dummy bits during VCCIO ramp up phase to enable correct setting of XTAL FREQ.	13.30.0.7095	A
LKF_A1_PMC_FW_133.0.01.1011	No Change	13.30.0.7099	A
LKF_A1_PMC_FW_133.0.01.1012	System gets woken via RTC while in Sx. Soft Strap Repull Sequence updated so system always boots from UFS.	13.30.0.1005	A

PMC Version	Changes	Firmware Version	Stepping Supported
	PCI Buffer control registers are configured correctly after exit from Cold reset.		
LKF_A1_PMC_FW_133.0.01.1013	Fix added for Platform to xDCI interface transactions functionality. PCI related debug registers for crashlog increased in byte size to display complete information.	13.30.0.1012	A
LKF_A1_PMC_FW_133.0.01.1013	No Change	13.30.0.1015	A
LKF_A1_PMC_FW_133.0.01.1013	No Change	13.30.0.1017	A
LKF_A1_PMC_FW_133.0.01.1014	Control of LP_HV rail optimized to enable Packaged C 10 state entry and exit under all conditions SVID ramp up event changed to earlier in boot sequence to allow for better Packages C10 exit states.	13.30.0.1019	A
LKF_A1_PMC_FW_133.0.01.1014	No Change	13.30.0.1023	A
LKF_A1_PMC_FW_133.0.10.1005	Modification in Dekel PHY Power -inaccessible entry sequence. Assertion of Power Good after a ramp up to 0.4 V to allow for no failures at boot up. Modified Date and Time algorithm to handle Hours Roll over to next day.	13.30.0.1023	B
LKF_A1_PMC_FW_133.0.10.1007	After boot the Clock is always tuned from Phase Locked Loop.	13.30.0.1030	B
LKF_A1_PMC_FW_133.0.01.1014	No Change	13.30.0.1031	A / B
LKF_A1_PMC_FW_133.0.10.1016	Unexpected RTC timeout during cycling testing resolved	13.30.0.1035	A / B
LKF_B0_B1_PMC_FW_133.0.10.1017	I2S Fast Speed Plus (FS+) configuration capability added. The speed values are optimized up to 730-760kHz	13.30.0.1042	B
LKF_B0_B1_PMC_FW_133.0.10.1019	Added PMC FW delay to resolve dekelPhy hang during warm reset cycling.	13.30.0.1047	B
LKF_B0_B1_PMC_FW_133.0.10.1025	Added PMC FW delay to resolve dekelPhy hang during warm reset cycling.	13.30.0.1048	B
LKF_B0_B1_PMC_FW_133.0.10.1025	No Change	13.30.0.1048	B
LKF_B0_B1_PMC_FW_133.0.10.1026	System gets hung when Type-C hub hot-plug during LPA (PMC in FW_MSG_IN_PROG loop)	13.30.0.1048	B
LKF_B0_B1_PMC_FW_133.0.10.1026	No Change	13.30.0.1048	B
LKFB1_B0_PMC_FW_133.0.10.1028	Firmware based S0ix block/break reason counter updated to meet telemetry requirements	13.30.0.1054	B
LKFB1_B0_PMC_FW_133.0.10.1031	PMC FW will stop timers earlier on S0ix flows	13.30.0.1060	B
LKFB1_B0_PMC_FW_133.0.10.1032	No Change	13.30.0.1062	B
LKFB1_B0_PMC_FW_133.0.10.1033	No Change	13.30.0.1065	B

PMC Version	Changes	Firmware Version	Stepping Supported
LKFB1_B0_PMC_FW_133.0.10.1034	No change	13.30.0.1065	B
LKFB1_B0_PMC_FW_133.0.10.1037	No change	13.30.0.1065	B

4.4 PFT Changes

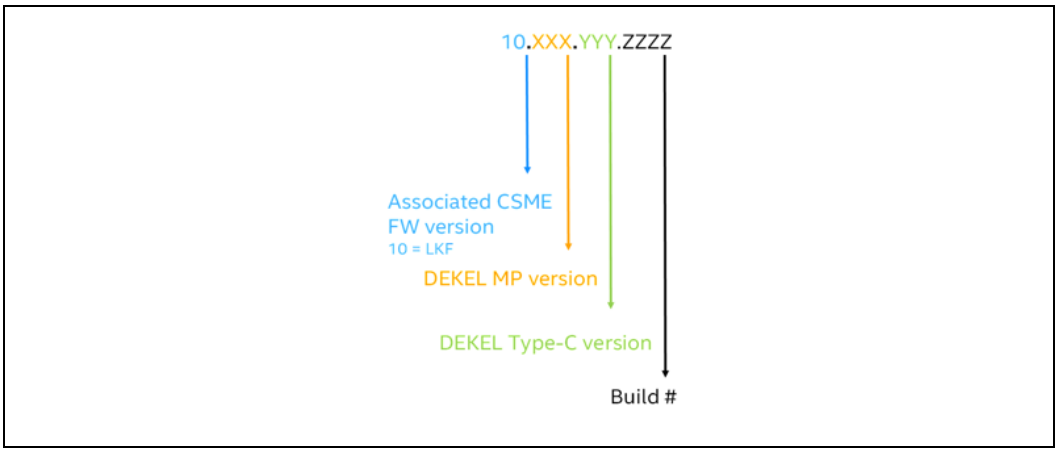
PFT Version	Changes	Firmware Version	Stepping Supported
5.8.7.2	Fix for yellow bang issue seen on the DnX driver.	13.30.0.7072	A
5.8.7.2	No Change	13.30.0.7073	A
5.8.8.0	Added Read command capabilities	13.30.0.7085	A
5.8.9.0	No Change	13.30.0.7087	A
5.8.9.0	No Change	13.30.0.7093	A
5.8.9.0	No Change	13.30.0.7095	A
5.8.9.0	No Change	13.30.0.7099	A
5.8.9.0	No Change	13.30.0.1005	A
5.9.0.0	DnX APIs from CSE FW kit 13.30.0.1012 integrated Secure token creation and injection flows implemented Read DnX commands implemented in CLI version of DnXFwdownloader tool New commands 'setcapabilities' and 'downloadoemkeymanifest' added both support "OEM authorization for opening DnX capabilities after EOM". To support the same "OEM authorization for opening DnX capabilities after EOM" a new setting "DnX Capabilities" was added to the OEM Unlock Token.	13.30.0.1012	A
5.9.0.0	No Change	13.30.0.1015	A
5.9.0.0	No Change	13.30.0.1017	A
5.9.0.0	No Change	13.30.0.1019	A
5.9.1.0	Fix for PT-3653 (BTG knob values not shown). "Cancel OEM Authentication". Upgraded SignFile to 4.0.78. Added feature to get device data from Binary file. Removed other tokens from drop down of PFT OEM except OEM tokens. Added ISH debug knob to Lakefield tokens: Intel unlock, OEM unlock token and IDLM unlock token Modification in OEM unlock token template. Added USBScanner utility to OEM version of PFT. XFSTK downloader support disabled.	13.30.0.1023	All
5.9.3.0	New knob for Intel® CSE Tracing added to all the platforms.	13.30.0.1031	All

PFT Version	Changes	Firmware Version	Stepping Supported
	New Knob Enable Debug Interface. Renaming of all the platform acronyms to full names. Changed the Boot Guard options as per the latest FW implementation and aligned it across all the platform in PFT except Broxton.		
5.9.3.0	No Change	13.30.0.1035	All
5.9.3.0	No Change	13.30.0.1042	All
5.9.4.0	Mismatch in Serial Number between USBScanner.exe and dnxFwDownloader.exe.	13.30.0.1047	All
5.9.4.0	No Change	13.30.0.1048	All
5.9.5.0	Upgraded openssl to 1.0.2t Integrated DnX Version 13.30.0.1052 Support for a new device type "ufs_hpb" has been added in dnxfwdownloader utility Added remaining flags for LKF whose position is set but are not being used	13.30.0.1054	All
5.9.5.0	No Change	13.30.0.1060	All
5.9.5.0	No Change	13.30.0.1062	All
5.9.5.0	No Change	13.30.0.1065	All

4.5 Dekel PHY Changes

Dekel PHY FW –Release Version Numbering Information

- Dekel PHY FW consists of Multi-PHY FW and Type C FW.
- Versioning of this FW follows Major.Minor.HF.Build scheme.



- **Major =** This field Generation support of Dekel PHY FW. This 2 digits for LKF is set to 10 indicating 1st generation.
- **Minor = XXX:** This 3 digits field represents the version of Multi-Phy FW embedded.
- **HF**= **YYY** – This 3 digits field represents the version of Type-C FW embedded.

  Build = **ZZZZ** – This 4 digit field represents the release/build version.

Dekel PHY Version	Changes	Firmware Version	Stepping Supported
LKFB1_A0_DEKEL_FW_PATCH_V1_5	Fix for calibration vector support for LKF Changes to support PM flows.	13.30.0.7072	A
LKFB1_A0_DEKEL_FW_PATCH_V1_5	No Change	13.30.0.7073	A
LKFB1_A1_DEKEL_FW_PATCH_V1_11	Fix added to handle lane reset Flow.	13.30.0.7085	A
LKFB1_A1_DEKEL_FW_PATCH_V1_15	Isolation mode scripts –dropped. Handling of PLL2 disable updated. Improved LFPS behavior. Vref flow behavior updated. Improved USB3 stability when handling multiple devices.	13.30.0.7087	A
LKFB1_A1_DEKEL_FW_PATCH_V1_21	Fixed added for PCIe3 and USB3.1 gen2 PSA settings.	13.30.0.7093	A
LKFB1_A1_DEKEL_FW_PATCH_V1_23	Fixed the DP to USB dynamic switching problem solved and tested.	13.30.0.7095	A

Dekel PHY Version	Changes	Firmware Version	Stepping Supported
	PCET timer from the FOM script set to 2ms per preset eval. Rate changes, ST1 values to improve BER issues discovered in PCIe Gen3 and Gear4 are added. Max coefficient value for DFE taps 3, 4, 5 and 6 is fixed at 102. VGA ST1 init value is loaded to 128. EHM HW configuration for CDR lock estimationtype fix.		
LKF_Dekel_FW_Patch_10.150.116.1024	DPX2 MFD issue resolved. Lane 1 hotplug resolved; LFPS Cal removed.	13.30.0.7099	A
LKF_Dekel_FW_Patch_10.150.116.1025	PCIe power gating disabled with this version. DSP code modified to help in training time and repeatability.	13.30.0.1005	A
LKF_Dekel_FW_Patch_10.150.116.1026	DSP code modified to help in training time and repeatability.	13.30.0.1005	A
LKF_Dekel_FW_Patch_10.184.117.1028	PG flow adding save and restore workaround fix. Lane flip workaround reverted back.	13.30.0.1012	A
LKF_Dekel_FW_Patch_10.118.184.1030	Enabled dynamic PG for MultiPHY. Enabled SRIS mode for MultiPHY. Fixed rate change calib skip vector (set fw_calib_support bit, calib ID 0). Broadcasting the rcomp code from cl to dl after vnn removal is added. Power Gating feature from G1 to G3 enabled for PCIe.	13.30.0.1012	A
LKF_Dekel_FW_Patch_10.119.193.1031	DSP code changes added to help in training time and repeatability. Changes added to PG flow for save and restore point. Added changes to resolve the UFS G4 failures with PG changes. Fix added to resolve S0ix support issue.	13.30.0.1015	A
LKF_Dekel_FW_Patch_10.119.193.1031	No Change	13.30.0.1017	A
LKF_Dekel_FW_Patch_10.119.193.1031	No Change	13.30.0.1019	A
LKF_Dekel_FW_Patch_10.119.193.1031	No Change	13.30.0.1023	A
LKF_Dekel_FW_Patch_10.0.203.1106	Fix for Sx/Warm reset entry issue	13.30.0.1023	B

Dekel PHY Version	Changes	Firmware Version	Stepping Supported
LKF_Dekel_FW_Patch_10.0.203.1107	Fixed additional DFE Tap2 calculated (didn't remove old line) Added static delay before each call of lane_req_handler in lane_flow. Removed unused interrupts in the common lane. Disabled some unused IRQs in CL.	13.30.0.1030	B
LKF_Dekel_FW_Patch_10.203.03.1032	No change	13.30.0.1031	A
LKF_Dekel_FW_Patch_10.0.203.1109	Fixed ctle: write into tx2_glue_lanex_tx_dword31 (att) 30 (boost).	13.30.0.1031	B
LKF_Dekel_FW_Patch_10.206.03.1113	Unable to link up to gen3 after gen3 EQ complete. TC Port 0 Gen3 x2 Equalization Seeing FOM 0x0 reported from back to back EQ test. phystatus is not toggling after rate change for lanes 1 and 2. ns_delay function in FW doesnt get executed all the time. Wifi port entering link recovery in L1.OFF with PHY DL PG enabled. With DLPG, link not able to enter L1sub after several iterations due to short L1 residency. rxclk is incorrect ; rx symbol errors.	13.30.0.1035	B
LKF_Dekel_FW_Patch_10.207.03.1114	NVME lost detection during warm reset	13.30.0.1042	B
LKF_Dekel_FW_Patch_10.208.80.1116	Chipset init configuraion is saved and restored during PM flows	13.30.0.1047	B
LKF_Dekel_FW_Patch_10.208.80.1119	After several warm resets, USB3 went to Inactive.	13.30.0.1048	B
LKF_Dekel_FW_Patch_10.208.80.1120	BugCheck CRITICAL_PROCESSOR_DIED, during S0ix cycles (Dump not generated (Stuck at 0%)	13.30.0.1048	B
LKF_Dekel_FW_Patch_10.208.80.1123	TypeC sidePOK not deasserted observed during WR/S5 cycling. Observing very bad S0I2.0 Residency (VNNAON) vs. S0I2.1 on same minimal hardware configuration.	13.30.0.1048	B
LKF_Dekel_FW_Patch_10.211.200.1125	Fixed observed CAT error during S4 cycles pointing to WWAN. Fixed USB3 device intermittently link speed drop to SS/HS during flip hotplugs regression. Fixed TypeC sidePOK not deasserted observed during WR/S5 cycling.	13.30.0.1048	B
LKF_Dekel_FW_Patch_10.211.200.1125	No Change	13.30.0.1054	B
LKF_Dekel_FW_Patch_10.214.203.1130	DFIA1_PLL_0/2 blocking S0ix entry during S0ix cycling	13.30.0.1060	B

Dekel PHY Version	Changes	Firmware Version	Stepping Supported
LKF_Dekel_FW_Patch_10.214.203.1132	LCPLL Blocking S0iX entry due to TCPLL	13.30.0.1062	B
LKF_Dekel_FW_Patch_10.214.203.1133	DKL FW 203plus11 is LCLL Fix for USB compliance.	13.30.0.1065	B
LKF_Dekel_FW_Patch_10.214.203.1134	NVME lost in WR, S4 NVME lost to EDK shell	13.30.0.1065	B
LKF_Dekel_FW_Patch_10.218.203.1136	USB Compliance fixes DKL FW 203plus11 is LCLL Fix	13.30.0.1065	B

4.6 PCHC Changes

PCHC Version	Changes	Firmware Version	Stepping Supported
LKF_A1_PCHC_FW_V7001	Fix for lpcll_dword0 supporting Ax stepping added.	13.30.0.7099	A
LKF_A1_PCHC_FW_V7001	No Change	13.30.0.1005	A
LKF_A1_PCHC_FW_V7001	No Change	13.30.0.1012	A
LKF_A1_PCHC_FW_V7002	Updated version for A1 stepping.	13.30.0.1012	A1 Only
LKF_A1_PCHC_FW_V7002	No Change	13.30.0.1015	A1 Only
LKF_A1_PCHC_FW_V7002	No Change	13.30.0.1017	A1 Only
LKF_A1_PCHC_FW_V7002	No Change	13.30.0.1019	A1 Only
LKF_A1_PCHC_FW_V7002	No Change	13.30.0.1023	A1 Only
LKF_A1_PCHC_FW_V7000	B-Step Initial release	13.30.0.1023	B0 Only
LKF_A1_PCHC_FW_V7000	No Change	13.30.0.1030	B0 Only
LKF_A1_PCHC_FW_V7002	No Change	13.30.0.1031	A1 Only
LKF_A1_PCHC_FW_V7000	No Change	13.30.0.1031	B0 Only
LKF_A1_PCHC_FW_V7002	No Change	13.30.0.1035	A1 Only
LKF_A1_PCHC_FW_V7000	No Change	13.30.0.1035	B0 Only
LKF_A1_PCHC_FW_V7000	No Change	13.30.0.1042	A and B
13.30.0.1005	Fix for LP HDA issue.	13.30.0.1054	B Only
13.30.0.1005	No Change.	13.30.0.1060	B Only
13.30.0.1005	No Change.	13.30.0.1062	B Only
13.30.0.1005	No Change.	13.30.0.1065	B Only

4.7 Intel® iCLS Changes

Intel® iCLS SW Version	Introduced in Intel® CSME SW version	Changes
1.55.66.0	1.55.66.0	• gSoap updated to 2.8.83 • SDK/WDK/ADK updated to 19H1 10.0.18362.0 (RTM)

Intel® iCLS SW Version	Introduced in Intel® CSME SW version	Changes
		• UWD INF installer certified for RS3,RS4,RS5&19H1

Note: Intel® Content License Service (iCLS) requires internet connectivity over TCP/IP port 443; if the port is blocked by the network, iCLS cannot communicate with the iCLS Service Servers.

5 Intel® CSE New Features RCR's

RCR #	Change Info	Status

6 Issue Status Definitions

This document provides sightings and bugs report for Intel® CSE Firmware 13.30 SKU for the LakeField Platform. At the time of a milestone release, this report is distributed with the Intel® CSE Kit and provides information on new issues and the status of old issues (replacing the Release Notes document).

Closed Issues: This category only displays closed issues within the current Intel® CSE Kit release. After each release, old issues are dropped down to the "Archive" section and then new closed issues takes its place back up top for the next release. If an issue is posted in this section, it indicates that the issue has been verified and fixed within the kit that is being released.

Known Issues: This category displays all Known Issues since the Alpha release and remains in this section until fixed or noted otherwise. "Known Issues" are still under investigation and may or may not be root caused.

Archive – Fixes in Previous Kits: This category displays all closed issues that were closed in their respected kit#. This section serves as a history of fixed issues.

Sightings listed in this document apply to the LakeField SKU's unless noted otherwise in this document or in the sightings tracking systems.

7 Closed Issues 13.30.0.1065

Issue #	Description	Details	Fixed in Kit #
1307227226	Intel® CSE reset when the RPMB counter is larger than 1 will result firmware being disabled.	**Affected Component –** fw.fw_os.storage **Impact:** Firmware **Workaround:** None	13.30.0.1062

8 Open / Known Issues to Date

Issue #	Description	Details	Found in Kit #

9 Archive Fixes in Previous Kits

9.1 Kit 13.30.0.1062

Issue #	Description	Details	Found in Kit #
1307069595	MEInfo returns Error 280 after 2-3 interations of Intel® CSE reset.	**Affected Component –** fw.bringup.host_comm **Impact:** MEInfo cannot retrieve data from Intel® CSE. **Workaround:** None	13.30.0.1060
1307114154	IDLM over UFS override ROM's storage context, as a result ROM can't load RBE and boot ends up in dnx triggering.	**Affected Component –** fw.debug.idlm **Impact:** IDLM not working as expected when UFS is the starage medium. **Workaround:** None	13.30.0.1060
1307116377	Intel® FIT tool fails to decompose an image dumped from a plaform.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT tool cannot decompose an image that has been dumped from a plaform. **Workaround:** None	13.30.0.1060

9.2 Kit 13.30.0.1060

Issue #	Description	Details	Found in Kit #
1306138412	Platform does not boot after power loss during FWUpdate.	**Affected Component –** fw.fw_os.storage **Impact:** Power loss during FWUpdate will result in platform not booting. **Workaround:** None	13.30.0.1054
1307020706	DnX module is not properly identifying close of manufacturing.	**Affected Component –** fw.dnx.dnx **Impact:** DnX is not identifying when close of manufacturing has been done on the platform. **Workaround:** None	13.30.0.1054
1307010691	DnX module is not able to communicate with unformatted UFS parts.	**Affected Component –** fw.dnx.dnx **Impact:** DnX is unble to communicate with unformatted UFS parts. **Workaround:** None	13.30.0.1054

Issue #	Description	Details	Found in Kit #
1307011339	DnX configpart command failing.	**Affected Component –** fw.dnx.dnx **Impact:** DnX configpart command failing to initialize the flag init_logical_partitions. **Workaround:** None	13.30.0.1054

9.3 Kit 13.30.0.1054

Issue #	Description	Details	Found in Kit #
1306810379	When the platform is in live unlock RTFD is not being disabled as expected.	**Affected Component –** fw.sku.bringup **Impact:** When the platform is in live unlock debugging mode RTFD (Return to Factory Defaults) is not being disabled as expected. **Workaround:** None	13.30.0.1048
1306998574	HDCP Rx enable flags are not correct in WiDi initialization.	**Affected Component –** fw.cp.hdcp_rx **Impact:** HDCP Rx enabled flags not be configured correctly during WiDi initialization. **Workaround:** None	13.30.0.1048
1307008064	DnX module is not checking if boot LUN is enabled.	**Affected Component –** fw.dnx **Impact:** DnX module is not checking to see if boot LUN has been enabled. **Workaround:** None	13.30.0.1048
1306977553	Platform hanging after firmware update.	**Affected Component –** fw.os.storage **Impact:** After firmware update the platform is not able to boot. **Workaround:** None	13.30.0.1048
1306576326	MEInfo sporadically reports Intel® CSE device not recognized after firmware reset flow.	**Affected Component –** fw.heci **Impact:** The MEInfo tool will intermitantly fails to get Intel® CSE status after firmware reset. **Workaround:** None	13.30.0.1048
1306635873	Return to factory defaults not working as expected on LKF with SPI.	**Affected Component –** fw.policy_manager.rtfd **Impact:** The return to factory default flow does not working as expected on LKF with SPI. **Workaround:** None	13.30.0.1048

Issue #	Description	Details	Found in Kit #
1306956311	MEManuf failing when ip loading RBE test is disabled.	**Affected Component –** fw.ip_loading.sphy **Impact:** When the ip loading RBE test is disabled the MEManuf tool will return Error 654. **Workaround:** None	13.30.0.1048

9.4 Kit 13.30.0.1048

Issue #	Description	Details	Found in Kit #
1306821366	DnX Config part command doesn't work when using high speed download.	**Affected Component –** fw.dnx **Impact:** DnX Config part command showing UFS errors when high speed download used. **Workaround:** None	13.30.0.1047
1507389661	MEInfo -fwsts and Intel® FPT -i command line options failing to work when FDO is asserted.	**Affected Component –** sw.mfg_tools.fpt; sw.mfg_tools.info **Impact:** Command MEInfo and Intel® FPT line options intended to work when FDO asserted are failing with Error 3 and Error 61. **Workaround:** None	13.30.0.1047
1306848288	Intel® FPT fails to disable the Intel® CSME when iTouch is enabled with no driver installed.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT does not disable Intel® CSME as expected when iTouch is enabled. **Workaround:** None	13.30.0.1047
1306832889	Intel® FPT failing to initialize the SPI interface with error 64.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT unable to initialize the SPI interface. **Workaround:** None	13.30.0.1047

9.5 Kit 13.30.0.1047

Issue #	Description	Details	Found in Kit #
1306708721	Missing ICC SDK DLL from External kits.	**Affected Component –** sw.mfg_tools.icc.sdk **Impact:** Required DLL file for the ICC not in kit. Customers would be unable to use the SDK. **Workaround:** None	13.30.0.1035

Issue #	Description	Details	Found in Kit #
1306808500	Bootguard enforcing timeouts on profile 0 on SPI and UFS.	**Affected Component –** fw.bootguard.boot_guard2.1 **Impact:** Timeout enforcement flows being excuted on profile 0. **Workaround:** None	13.30.0.1035

9.6 Kit 13.30.0.1042

Issue #	Description	Details	Found in Kit #
1306732701	MEManuf -S0 test returns error 655: Loading test generic error	**Affected Component –** sw.mfg_tools.manuf **Impact:** MEManuf with –S0 command line option sporadically fails with "Error 655: Loading test generic error" **Workaround:** None	13.30.0.1035
1306743220	Intel® CSE firmware (UFS) ignores DCI Enabled setting.	**Affected Component –** fw.rbe **Impact:** The UFS version Intel® CSE firmware ignores the DCI enabled setting. **Workaround:** None	13.30.0.1035
1306659658	Target Type in the Intel® FIT tool is not updating when loading XML.	**Affected Component –** sw.mfg_tools.fit **Impact:** The Target Type is not being updated when switching between UFS and SPI XML files. **Workaround:** None	13.30.0.1035
1306671510	The platform does not enter into S5/S4/warm reset/global reset from OS level when using MEI driver later than 13.30.0.1031.	**Affected Component –** fw.rbe **Impact:** Platform cannot enter any Sx states proper when using MEI drivers newer than 13.30.0.1031. **Workaround:** Use 13.30.0.1031 MEI driver or disable MEI driver in device manager.	13.30.0.1035
1306685859	Platform will not boot to OS after a GLOBAL RESET.	**Affected Component –** fw.rbe, fw.pm.pmc_patch, fw.pm.maestro **Impact:** Platform unable to boot after going through a Global Reset. **Workaround:** None	13.30.0.1035

9.7 Kit 13.30.0.1035

Issue #	Description	Details	Found in Kit #
1306482618	Intel® MEU returning unexpected error message 394 being returned when an unsupported 3k private key is used.	**Affected Component** – sw.mfg_tools.meu **Impact:** Intel® MEU returns confusing error message when a 3k private key not supported on LKF is used. **Workaround:** None	13.30.0.1031

9.8 Kit 13.30.0.1031

Issue #	Description	Details	Found in Kit #
1306136694	DnX fails to read RPMB partition after provisioning.	**Affected Component –** fw.dnx **Impact:** DnX not able to read all partitions as expected. **Workaround:** None	13.30.0.1030
1306231215	FWUpdate fails when "IfwiRedundancyEnabled" is set to "No" for the SPI image built with the Intel® FIT tool.	**Affected Component –** sw.mfg_tools.fit **Impact:** FWUpdate will fail with error 336 when the SPI image has been built in the Intel® FIT tool with "IfwiRedundancyEnabled" set to "No". **Workaround:** None	13.30.0.1030
1409198356	EFI MEInfo hangs if PAVP is disabled.	**Affected Component –** sw.mfg_tools.info **Impact:** The EFI version of MEInfo hangs if PAVP is disabled when it calls IsKeyboxProvisioned(). **Workaround:** None	13.30.0.1030
1807324234	Intel® FPT crashing when trying to perform a blank check after erase (FPT -b -verbose).	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT crashes when the blank check command is used. **Workaround:** None	13.30.0.1030
1807363374	The PCHC version is not displayed in the Intel® FIT tool.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT does not display the PCHC version as expected. **Workaround:** None	13.30.0.1030

9.9 Kit 13.30.0.1030

Issue #	Description	Details	Found in Kit #
1305732310	Prevent EOM flows when Bootguard profile 3 is selected.	**Affected Component –** fw.bootguard.boot_guard2.1 **Impact:** Since Bootguard profile 3 is only meant for debugging EOM flows should be prevented if this profile is configured. **Workaround:** Switch to one of the valid Bootguard profiles on production images.	13.30.0.1023
1305440257	Intel® FPT –closemnf command should block commit_to_fpf command for RPMB capable boot devices.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT –closemnf command causes FPFs commit on RPMB capable boot devices which results in errors during RPMB provisioning. **Workaround:** None	13.30.0.1023
1306056160	Manufacturing tools fail with - Error 273: Used an invalid input parameter to access the NVAR file.	**Affected Component –** sw.mfg_tools.fpt sw.mfg_tools.info sw.mfg_tools.manuf **Impact:** Manufacturing tools fail with Error 273: Used an invalid input parameter to access the NVAR file. **Workaround:** None	13.30.0.1023
1306118936	The ICC Get Mphy command is not functional.	**Affected Component –** fw.icc.chipset_init_flow **Impact:** Using the ICC Get Mphy command will return Error 3: Internal Error. Unexpected error occurred. **Workaround:** None	13.30.0.1023
1306119760	ISH trace log read/write in Pre-OS/Post OS from UFS storage.	**Affected Component –** fw.ip_loading.ish **Impact:** ISH logging not working as expected. **Workaround:** None	13.30.0.1023
1306136446	Intel® FIT tool missing EOM on first boot setting for UFS.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT does not have EOM setting for UFS. **Workaround:** None	13.30.0.1023
1306169246	LKF doesn't boot after provisioning RPMB.	**Affected Component –** fw.mfg_fw.rpmb **Impact:** The platform fails to boot after RPMB provisioning. **Workaround:** None	13.30.0.1023

Issue #	Description	Details	Found in Kit #
1306186798	Intel® MEU does not build DnX IFWI if signing tool (openSSL) is disabled	**Affected Component –** sw.mfg_tools.fit sw.mfg_tools.meu **Impact:** Intel® MEU errors out when signing is disabled. **Workaround:** None	13.30.0.1023
1306230465	On LKF platform, over UFS, when enabling DAM on the fit first boot is in DAM mode but after G3 platform goes back to lock and CSE gets stuck.	**Affected Component –** fw.os.storage **Impact:** DAM is not staying enabled after platform G3. **Workaround:** None	13.30.0.1023

9.10 Kit 13.30.0.1023

Issue #	Description	Details	Found in Kit #
1306172391	Replacing the Intel® CSE binary through CLI using switch option fails.	**Affected Component –** sw.mfg_tools.fit **Impact:** Replacing Intel® CSE binary through the command line interface using the switch option fails and returns error 212. **Workaround:** Change the Intel® CSE binary through the XML file.	13.30.0.1017
1305542268	'Get Clock' API is not working and returns with FAILURE.	**Affected Component –** fw.icc.clocking **Impact:** Unable to read clock values back when using the API. **Workaround:** None	13.30.0.1017

9.11 Kit 13.30.0.1019

Issue #	Description	Details	Found in Kit #
1306295877	MEManuf failing FPFs on with EOL config check prior to platform EOM.	**Affected Component –** sw.mfg_tools.manuf **Impact:** MEManuf showing FPF mismatch errors when EOL config check is run prior to platform end of manufacturing being set. The correct behavior should be to indicate that FPFs have not been committed. **Workaround:** None.	13.30.0.1017

9.12 Kit 13.30.0.1017

Issue #	Description	Details	Found in Kit #
1306078554	MEU should support building DnX image without OEM KM.	**Affected Component –** sw.mfg_tools.meu **Impact:** MEU will not allow images DnX images to be built with OEM KM present. **Workaround:** None.	13.30.0.1015
1306135678	Creating full FWU image fails on partition size.	**Affected Component –** sw.mfg_tools.fit **Impact:** FIT tool not building full FWU images. **Workaround:** None.	13.30.0.1015

9.13 Kit 13.30.0.1015

Issue #	Description	Details	Found in Kit #
1306230465	UFS system fails to boot with DAM enabled through the Intel® FIT tool.	**Affected Component –** fw.os.storage **Impact:** On first boot DAM is enabled but after G3 the platform goes back to lock mode and the Intel® CSE gets stuck. **Workaround:** None.	13.30.0.1012
1306241169	GReset not happening as expected when DAM is enabled through BIOS.	**Affected Component –** fw.policy_manager_mkhi **Impact:** Platform not going through GReset preventing DAM from working. **Workaround:** None.	13.30.0.1012

9.14 Kit 13.30.0.1012

Issue #	Description	Details	Found in Kit #
1306186798	Intel® MEU tool does not build DnX image if signing tool (openssl) is disabled.	**Affected Component –** sw.mfg_tools.meu **Impact:** The Intel® MEU tool would not build the DnX image if signing tool option is set to disabled. **Workaround:** None.	13.30.0.1005
1306191270	FW reset without failure mode causes Intel® PTT to not respond to locality request.	**Affected Component –** fw.ptt.bringup **Impact:** Intel® PTT fails to respond to requests. **Workaround:** None.	13.30.0.1005

Issue #	Description	Details	Found in Kit #
1306136446	Intel® FIT tool missing End of Manufacturing Enable option for UFS.	**Affected Component –** sw.mfg_tools.fit **Impact:** There is no way to configure automatic EOM through the Intel® FIT tool for UFS. **Workaround:** None.	13.30.0.1005
1405928161	Critical flash log message written when Intel® CSE does not have access to UFS are lost.	**Affected Component –** fw.os.storage **Impact:** When Intel® CSE is not able to access UFS flash any critical flash log message that occur during that time is lost. **Workaround:** None.	13.30.0.1005

9.15 Kit 13.30.0.1005

Issue #	Description	Details	Found in Kit #
1306031498	FPT show warning without error when performing closemnf over UFS when the Intel® CSE driver is disabled.	**Affected Component –** sw.mfg_tools.fpt **Impact:** FPT unable to access the UFS storage device when Intel® CSE driver is disabled. **Workaround:** None.	13.30.0.1005
1606881679	Unable to unlock the part by LTB with DAM Enabled.	**Affected Component –** firmware **Impact:** Unlocking issue seen when DAM is set to enable. **Workaround:** None.	13.30.0.1005
1408132722	FPT and MEInfo tools causes BSOD "stop code: WDF Violation" when executed in Windows* RS5. EFI Shell works ok.	**Affected Component –** sw.mfg_tools.fpt Sw.mfg_tools.info **Impact:** FPT and MEInfo tools causing BSOD issues. **Workaround:** None.	13.30.7087

9.16 Kit 13.30.0.7099

Issue #	Description	Details	Found in Kit #
1306078554	Intel® MEU tool does not support building DnX image without OEM KM.	**Affected Component –** sw.mfg_tools.meu **Impact:** Intel® MEU would not build DnX images without the OEM KM. **Workaround:** None.	13.30.0.7095

Issue #	Description	Details	Found in Kit #
1305534942	Intel® DAL can potentially fail while trying to save firmware update data when SVN is incremented.	**Affected Component –** fw.dal.management **Impact:** Intel® DAL could fail during firmware update with SVN being done. **Workaround:** None.	13.30.0.7095

9.17 Kit 13.30.0.7095

Issue #	Description	Details	Found in Kit #
1305950032	DNX module crashes on RpmbGetCounter when burning UFS via DNX with RPMB not provisioned.	**Affected Component –** fw.dnx **Impact:** DNX module crashes when attempting to flash UFS using DNX. **Workaround:** None.	13.30.0.7093
1306031498	Intel® FPT shows a warning error when performing closemnf over UFS when MEI driver is disabled.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT not able to complete closemnf flow on UFS. **Workaround:** None.	13.30.0.7093

9.18 Kit 13.30.0.7093

Issue #	Description	Details	Found in Kit #
1305948091	Remove all output data not relevant to LakeField platforms.	**Affected Component –** sw.mfg_tools.info **Impact:** Non-relevant output data being displayed. **Workaround:** None.	13.30.0.7087
1407916582	DNX getcardinfo fails to read attributes on UFS2.1 device.	**Affected Component –** sw.dnx **Impact:** The user unable to retrieve the proper UFS 2.1 attributes. **Workaround:** None.	13.30.0.7087
1506780016	DnX Module does not read / dump data from the LUNs.	**Affected Component –** fw.dnx **Impact:** The User would be unable to read/dump any data from the LUNs. **Workaround:** None.	13.30.0.7087
1305947997	Device initialization failure on entering DnX through corrupted boot critical component Intel® CSE region.	**Affected Component –** fw.dnx **Impact:** DnX fails to initialize with corrupted Intel® CSE. **Workaround:** None.	13.30.0.7087

Issue #	Description	Details	Found in Kit #
1305947989	LIBUSB_ERROR_Timeout on initiating DnX through GPIO.	**Affected Component –** fw.dnx **Impact:** DnX fails with LIBUSB_ERROR_Timeout when going through GPIO. **Workaround:** None.	13.30.0.7087
1305908856	MEInfo displays "Unknown" value for some SVN features.	**Affected Component –** fw.mfg_fw.mca **Impact:** MEInfo returning "Unknown" when outputting status on some SVN features. **Workaround:** None.	13.30.0.7087

9.19 Kit 13.30.0.7087

Issue #	Description	Details	Found in Kit #
2205441969	DNX module enters an error state if LUN1 does not have a valid Intel® CSE pointers table.	**Affected Component –** fw.dnx **Impact:** When entering DNX mode booting from to UFS and the first 4K LUN1 does not have a valid pointers table, DNX module's DNX storage init fail, causing all the NVM related commands to return an error and fail. **Workaround:** None.	13.30.0.7085

9.20 Kit 13.30.0.7085

Issue #	Description	Details	Found in Kit #
1806103951	LakeField 13.30.0.7072 installer fails to install SPD driver.	**Affected Component –** ip.installer.cse **Root Cause:** Installation order changed. **Symptoms:** Installer not working as expected. **Workaround:** Manual installation.	13.30.0.7085
1305712769	Intel® MEInfo shows Anti Rollback value as Unknown.	**Affected Component –** fw.mfg_fw.mca **Root Cause:** Buffer size of SVN counter variable changed. **Symptoms:** Anti Rollback status not being displayed correctly. **Workaround:** None.	13.30.0.7085

Issue #	Description	Details	Found in Kit #
1305453716	HECI failing to remove PG override, blocking CM0-PG entry.	**Affected Component –** fw.heci **Root Cause:** Not a bug. **Symptoms:** Platform unable to enter CM0-PG. **Workaround:** None.	N/A
1806147558	Warm / Cold reset causing PRTC to be cleared.	**Affected Component –** fw.pm.driver **Root Cause:** Issue moved to Simics **Symptoms:** PRTC unexpectedly being cleared after Warm / Cold resets. **Workaround:** None.	N/A
1305895994	MEInfo returns "Unexpected result in command response" error.	**Affected Component –** sw.mfg_tools.info **Root Cause:** Feature failure error response changed. **Symptoms:** Unclear error response confusing to users. **Workaround:** None.	13.30.0.7085
1305786460	ICC profile containing incorrect data.	**Affected Component –** sw.mfg_tools.fit **Root Cause:** ICC profile information updated for LakeField chipset. **Symptoms:** When the command get clock via CCT tool is executed the following error message gets displayed "ICC_status_unvalid_profile". **Workaround:** None.	13.30.0.7085
1305476646	Firmware update fails with error message "Firmware update tool failed to get the firmware parameters" on UFS.	**Affected Component –** fw.os.storage **Root Cause:** Not a bug. **Symptoms:** Firmware update currently not working on UFS. **Workaround:** None.	N/A

9.21 Kit 13.30.0.7073

Issue #	Description	Details	Found in Kit #
1305500208	Intel® CSE Boot ROM is waiting ~25 minutes before returning UFS device not present in cases where the device is missing.	**Affected Component –** fw.rom **Impact:** Intel® CSE Boot ROM not immediately responding when the UFS device not present. **Workaround:** None.	13.30.0.7073

Issue #	Description	Details	Found in Kit #
1305558349	Intel® CSE Boot ROM using incorrect location for power state field when putting UFS into D0 state.	**Affected Component –** fw.rom **Impact:** Intel® CSE Boot ROM not setting UFS to D0 state as expected. **Workaround:** None.	13.30.0.7073
2203280508	DnX settings are lost when decomposing an image in the Intel® FIT tool.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT tool does not retain DnX settings on decomposed images. **Workaround:** None.	13.30.0.7073

9.22 Kit 13.30.0.7072

Issue #	Description	Details	Found in Kit #
1806127895	DnX WriteToken not working the command is getting stuck.	**Affected Component –** fw.dnx **Impact:** Unable to use DnX WriteToken command. **Workaround:** None.	13.30.0.7072
1305712372	Configuring blank UFS part does not work. The command returns success while however the partitions still remains invalid.	**Affected Component –** fw.dnx **Impact:** Unable to configure blank UFS part through DnX. **Workaround:** None.	13.30.0.7072

10 Archive - Intel® CSE RCR's

RCR #	Change Info	Implemented in Kit#
1306152941	**Description:** Move AddComponent from OemExention to HECI.inf **Background:** To get other the drivers installed, OEM Ext INF needs to be installed on the system. OEM Ext describes the Hardware IDs that it supports and the components IDS that need to be installed on the system. The problem is in Windows Update, since we are using 2 Part Hardware IDs, Intel cannot push the OEM Ext to End User directly.	13.30.0.1030
1306184557	**Description:** Intel® FIT tool to support configuring BCLK frequency and Spread Spectrum Clock. **Background:** In Lakefield the register offsets and register structures changed from previous projects.	13.30.0.1030
1409235028	**Description:** Enable UFS ConfigLocking by DnX. **Background:** UFS spec supports ConfigLock (bConfigDescrLock) parameter to prevent write configuration at run time. It is a onetime operation after which re-configuration is not possible.	13.30.0.1030
1407610505	**Description:** Implement FwUpdate function to block end-users from successfully doing a firmware update of both FW and any of the IUP's. **Background:** Many OEMs have a strict policy of control over the full FW/SW stack installed on their platforms. No end-user should have descriptor access by any means. This trust boundary is to ensure their platforms' stability and security by allowing only versions the OEM approves. This of course includes CSME FW and the IUP's.	13.30.0.1030
1305660960	**Description:** Enable collection of North Peak trace information through MTB. **Background:** Early trace messages from PMC and CSE can be collected using BSSB only. If USB2.DbC is used as a debug interface than early trace messages are lost.	13.30.0.1023
1306067660	**Description:** Implement RPMB support in manufacturing tools. **Background:** RPMB support in APL is not fully aligned with latest design changes introduced in ICL and therefore some requirements' clarification is required.	13.30.0.1023
1306183927	**Description:** Improve the DnX UI in the Intel® FIT tool. **Background:** As part of the LKF project some of the requirements for DNX changed which impacts the Intel® FIT tool. Additionally this RCR provides simplifications Intel® FIT UI to provide a better user experience.	13.30.0.1023
1306067660	**Description:** Align RPMB support in tools on Lakefield with current implementation on Ice Lake. **Background:** Lakefield tools support for RPMB was not fully implemented.	13.30.0.1019

RCR #	Change Info	Implemented in Kit#
1407610505	**Description:** Implement FwUpdate function to block end-users from successfully doing a firmware update of both FW and any of the IUP's. **Background:** Some OEMs have strict policies of control over the full FW/SW stack installed on their platforms. This is to ensure their platforms' stability and security by allowing only versions the OEM has approved.	13.30.0.1019
1305559706	**Description**: ICC to consume the PCH configuration data from a new Sub-Partition. **Background**: Change to reduce the dependency between the PCH and Intel® CSE.	13.30.30.7093
1405745543	**Description**: Certify Intel® PTT to FIPS 140-2 Level 1 Standard. **Background**: Currently Intel® PTT does not support FIPS140-2 Level 1. This prevents Intel® PTT solution to be certified. In addition to missing the certification, no customer can use Intel® PTT for Secure Accounts (IE: Government Accounts).	13.30.30.7087
1305613719	**Description**: Remove System Integrator ID. **Background**: No longer required for functionality by iCLS and DAL.	13.30.30.7085
1305720367	**Description**: Remove automatic activation of DAM as a result of connecting CCA. **Background**: DAM allows to make system ready for debugging while authentication of the user can happen at any time. DAM is useful for Run Control debugging, but it changes behavior of multiple components in CSE FW. For better support of debugging the customers' platforms returned by the end users DAM is activated automatically on CCA connection.	13.30.30.7085
1406385434	**Description**: Have manufacturing tools return appropriate error and system ERRORLEVEL. **Background**: Currently when manufacturing tools report error, system ERRORLEVEL always shows 0x1. OEMs are requesting error handling logic to programmatically respond with an appropriate error and system ERRORLEVEL from the manufacturing tool.	13.30.30.7085
1806138045	**Description**: Add Intel® FIT tool support for manifest version validation. **Background**: Having Intel® FIT do validation on the IUPs listed in the manifest helps avoid during image build and or platform execution.	13.30.30.7085
1504626801	**Description**: Add ISH PDT version information for Capsule Update. **Background**: There is currently no support for reading either the PDT version, nor the Vendor-defined Data Version (VDV) for the currently installed PDT via BIOS to facilitate the Capsule Update process.	13.30.30.7085