IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DPH-I/T/TQ**
Release Version	**3.0c SPS: 04.1.4.256**
Release Date	**03/28/2018**
Previous Version	**3.0a**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated Intel BKCWW10 2019 PV MR3.** **2. Updated SPS_E5_04.01.04.256.0 from BKC WW08 2019.** **3. Updated SINIT ACM 1.7.2 PW from BKC WW06 2019.** **4. Updated Skylake-SP/Cascade Lake-SP CPU microcode from SRV_P_272.** **5. Hid Driver Health page for SUM.** **6. Reduced redundant reboot for offboard VGA switching.** **7. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.** **8. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.** **9. Enhanced BIOS setup menu to switch the boot mode value and Option ROM's values when CSM support is disabled and applied this to enabled secure boot mode case.**

New features	**N/A**
Fixes	**1. Fixed problem of the system equipped with dTPM 2.0 hanging up at POST code 0x90 when disabling dTPM 2.0 by SUM TPM OOB command "--disable_dtpm".** **2. Corrected TPM RSD ChangeTPMState behavior to control TPM 1.2/2.0 state instead of "Security Device Support".** **3. Fixed problem of TPM 2.0 device disappearing when disabling "RSD PSME ChangeTPMState API" and then enabling TPM 2.0 state.** **4. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.** **5. Fixed problems of system hanging up at POST code 0x92 and rebooting endlessly during POST and inability to get PPIN under OS (DOS/EFI shell/Windows/Linux).** **6. Fixed failure to log memory UCE event due to incorrect flag.** **7. Fixed inability of "Network Stack"-related items to get/change via SUM OOB method.** **8. Fixed incorrect display of the TDP of Intel Speed Select table.** **9. Patched problem of incorrect memory power being reported in PTU.** **10. Applied workaround for inability of SUM to get full setting of IODC setup item.** **11. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.** **12. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.**

Release Notes from Previous Release(s)

3.0a (1/24/2019)

1. Added support for Purley Refresh platform.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
3. Added 2933 to memory POR.
4. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
5. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
6. Updated CPU microcode SRV_P_262 for Skylake-SP H0/M0/U0 CPUs.
7. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
8. Added support for Linux built-in utility efibootmgr.
9. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.
10. Corrected standard NVDIMM ADR time.
11. Fixed incorrect PBF high frequency core number when Hyper-Threading is disabled.
12. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").

2.1 (6/15/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.
3. Updated 5.12_PurleyCrb_0ACFD087Beta for Purley Skylake platform PLR6, BKC 2018 WW14.
4. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.
5. Corrected BIOS/ME downgrade check for SPS 4.0.4.340.
6. Added SMC_BUS_MASTER_EN token for enabling SMC Bus Master or AMI DMA AMI BME DMA Mitigation in setup.
7. Updated Giga LAN EFI driver 8.3.0.4 (IBA 23.1).
8. Added support for UEFI mode PXE boot of F12 hot key Net boot.
9. Added support for RFC3021.
10. Corrected default setting for Enable SmcBusMasterEn setup item.
11. Checked PCH SKU for QAT enabled board.
12. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.
13. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.
14. Fixed problem of DMI being lost if DMI is changed and then UpdateBios is run.
15. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.
16. Fixed failure of WDT function.

2.0b (2/27/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.
3. Updated Purley RC 151.R03.
4. Updated BIOS ACM 1.3.5 and SINIT ACM 1.3.3.
5. Changed PCH uplink CTLE/VGA/TSM SI setting to [4,10,32].
6. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.

7. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.
8. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
9. Fixed issue with IPMI force boot.
10. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
11. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
12. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.
13. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
14. Fixed problem of the system not logging memory errors upon injection without rebooting.
15. Fixed inability of BIOS to boot into OS with Intel P3608 PCIe NVMe drive installed.

2.0a (12/16/2017)

1. Updated CPU microcode SRV_P_217 for Skylake-EP H0/M0/U0 stepping CPUs.
2. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
3. Fixed problem of the system not logging memory errors upon injection without rebooting.
4. Fixed inability to boot into OS that's installed on Intel P3608 PCIe NVMe drive.

2.0 (11/30/2017)

1. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.3.0.1052.
2. Updated the onboard X722 Lan NVM to 722PAD1C.
3. Reduced the boot time caused by IPv4/IPv6 polling.
4. Updated BIOS ACM 1.3.4.
5. Added support for AOC-SLG3-2M2 rev. 1.00 AOC cards (M.2 Riser Card).
6. Updated SPS 4.00.04.294 PLR 3.1 PV version.
7. Updated CPU microcode SRV_P_214 for Skylake-EP H0/M0/U0 stepping CPUs.
8. Updated 5.12_PurleyCrb_0ACFD084_BETA for Purley Skylake platform PLR 3.1.
9. Fixed failure of the IIO Root port PCIe manual bifurcation.
10. Fixed problem of system rebooting endlessly when equipping dTPM module.
11. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.