Intel® Server Platform Services Manageability Engine Firmware for Lewisburg Product Line Full, SiEn

Customer Release Notes

PLR1 Release for Purley Platforms

Document Version 1.0

July 2017

Contents

1 Introduction **5**
1.1 Revision Numbers of SPS Package Components 5

2 SPS Package Contents **8**

3 New/Changed Features **11**
3.1 New/Changed Features 11
3.2 Limitations 11
3.3 XML Changes 13
3.4 Documentation Updates 14

4 Known Issues **15**

5 Fixed Issues **16**

List of Tables

1.1 Revision numbers of PLR1 release components included in SPS_E5_04.00.03.235.0.zip package. 5
1.2 Revision numbers of PLR1 release components included in SPS_EPO_04.00.03.235.0.zip package. 5
1.3 Revision numbers of PLR1 release components included in SPS_Tools_4.2.68.50.zip package. 6
1.4 Revision numbers of PLR1 release components included in SPS_Tools_4.2.61.89_epo.zip package. 6
1.5 Revision numbers visible in component properties, on the console, or over IPMI included in SPS_E5_04.00.03.235.0.zip package. 6
1.6 Revision numbers visible in component properties, on the console, or over IPMI included in SPS_EPO_04.00.03.235.0.zip package. 7
1.7 Revision numbers visible in component properties, on the console, or over IPMI included in SPS_Tools_4.2.68.50.zip package. 7
1.8 Revision numbers visible in component properties, on the console, or over IPMI included in SPS_Tools_4.2.61.89_epo.zip package. 7

2.1 Software package 8

3.1 Current SPS Firmware Documentation. 14

4.1 Disposition field definition. 15
4.2 Known Issues. 15

5.1 Disposition field definition. 16
5.2 Fixed Issues. 16

1. Introduction

These release notes are intended for the PLR1 release of the Intel® Server Platform Services Manageability Engine Firmware for the Lewisburg Product Line.

The product name is abbreviated to SPS in the remainder of this document.

SPS Firmware for Purley platform can be configured in 2 different SKUs: Full, SiEn. Please refer to Intel® SPS External Product Specification [555192] for information regarding the Firmware SKU definition.

1.1. Revision Numbers of SPS Package Components

Table 1.1: Revision numbers of PLR1 release components included in SPS_E5_04.00.03.235.0.zip package.

Subproject (component)	Location	Revision
Intel(R) SPS ME Firmware	/spsOperational.bin	SPS_E5_04.00.03.235.0
Intel(R) SPS ME Recovery Boot Loader	/spsRecovery.bin	SPS_E5_04.00.03.235.0
Intel Flash Image Tool for Server Platform Services only	/Tools/FlashImageTool	SPS_E5_04.00.03.235.0

Table 1.2: Revision numbers of PLR1 release components included in SPS_EPO_04.00.03.235.0.zip package.

Subproject (component)	Location	Revision
Intel(R) SPS ME Firmware	/spsOperational.bin	SPS_E5_04.00.03.235.0
Intel(R) SPS ME Recovery Boot Loader	/spsRecovery.bin	SPS_E5_04.00.03.235.0
Intel Flash Image Tool for Server Platform Services only	/Tools/FlashImageTool	SPS_EPO_04.00.03.235.0

Table 1.3: Revision numbers of PLR1 release components included in SPS_Tools_4.2.68.50.zip package.

Subproject (component)	Location	Revision
Intel® Flash Programming Tool	/FlashProgrammingTool	SPS_Tools_4.2.68.50
SPS ME SMBus Diagnostic Console	/MeDiagnosticConsole	SPS_Tools_4.2.68.50
SPS ME SMBus Diagnostic Console	/MeDiagnosticConsoleAgent	SPS_Tools_4.2.68.50
Intel® ME Info with support for SPS	/SpsInfo	SPS_Tools_4.2.68.50
SPS FW Manufacturing Tool	/SpsManuf	SPS_Tools_4.2.68.50
Sample Update Tool for SPS	/SampleUpdateTool	SPS_Tools_4.2.68.50
NULL Heci Driver	/NullHeciDriver	SPS_Tools_4.2.68.50
Compliance Tests IPMI Tool Scripts	/ComplianceTestsScripts	SPS_Tools_4.2.68.50

Table 1.4: Revision numbers of PLR1 release components included in SPS_Tools_4.2.61.89_epo.zip package.

Subproject (component)	Location	Revision
SPS ME SMBus Diagnostic Console	/MeDiagnosticConsole	SPS_Tools_4.2.61.89_epo

Table 1.5: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_E5_04.00.03.235.0.zip package.

Console-Component	Revision
ME SPS Firmware Get Device Id response	50 01 04 03 02 21 57 01 00 0A 0B 04 23 50 01
ME SPS Recovery Boot Loader Get Device Id response	50 01 84 03 02 20 57 01 00 0A 0B 00 23 50 00
HECI MKHI_GET_FW_VERSION response	04.00.03.235
spsFITc.exe	4.0.3.235
SPS NM PTU option ROM SHA-256 hash to support UEFI Secure Boot Root Cert: Purley_SpsNMPTU_root.cer File: Purley_SpsNMPTU_signed.rom DB Cert: Purley_SpsNMPTU_signer.cer	1.5 A5 A5 4D FF B3 10 EB 02 C6 37 B9 72 6F F4 63 F0 D2 9C AD 0B 36 A2 17 01 17 32 26 44 8D 07 DC 2D

Table 1.6: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_EPO_04.00.03.235.0.zip package.

Console-Component	Revision
ME SPS Firmware Get Device Id response	50 01 04 03 02 21 57 01 00 0c 0b 00 23 50 01
ME SPS Recovery Boot Loader Get Device Id response	————————
HECI MKHI_GET_FW_VERSION response	04.00.03.235
spsFITc.exe	4.0.3.235

Table 1.7: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_Tools_4.2.68.50.zip package.

Console-Component	Revision
spsFPT.efi, spsFPTW64.exe	SPS_Tools_4.2.68.50
MESDC.exe	SPS_Tools_4.2.68.50
RemoteAgentLinux64, RemoteAgentWin64.exe	SPS_Tools_4.2.68.50
spsInfoWin64.exe, spsInfoLinux64, spsInfo.efi	SPS_Tools_4.2.68.50
spsManufWin64.exe, spsManuf.efi, spsManufLinux64	SPS_Tools_4.2.68.50

Table 1.8: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_Tools_4.2.61.89_epo.zip package.

Console-Component	Revision
MESDC.exe	SPS_Tools_4.2.61.89_epo

2. SPS Package Contents

Table 2.1 lists the contents of the release package.

Note: All of this software needs Intel® compatible PC with Microsoft Windows 7® x64, Microsoft Windows 8.1® x86/x64, Microsoft Windows 10® x64, Microsoft Windows Server 2012® R2 SP1 x64 or Microsoft Windows Server 10® x64 operating system installed depending on the specific tool requirements listed below.

Note: The release package contains one license file placed in the main directory. This license is specified for PLR1 release firmware.

Table 2.1: Software package

No.	Package	Contents
1	ReleaseNotes.pdf	This file.
2	Tools User Guide.pdf	User Guide for Tools package.
3	SPS_E5_04.00.03.235.0	This is a release package with Intel SPS ME Firmware and Tools for Lewisburg platform. Uncompress the package. The package will uncompress into SPS_E5_04.00.03.235.0 directory. SPSOperational - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory. SPSRecovery - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory. Intel Flash Image Tool for Server Platform Services only - Microstoft Windows* tool: This is a tool to create SPI Flash image and to modify SPS Firmware factory configuration. This tool is unpacked into the /Tools/FlashImageTool directory with dedicated license.

Table 2.1: Software package

No.	Package	Contents
4	SPS_EPO_04.00.03.235.0	This is a release package with Intel SPS ME Firmware and Tools for Lewisburg Endpoint Only platform. Uncompress the package. The package will uncompress into SPS_EPO_04.00.03.235.0 directory. SPSOperational - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory. SPSRecovery - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory. Intel Flash Image Tool for Server Platform Services only - Microstoft Windows* tool: This is a tool to create SPI Flash image and to modify SPS Firmware factory configuration. This tool is unpacked into the /Tools/FlashImageTool directory with dedicated license.
5	SPS_Tools_4.2.68.50	This is a release package with Intel SPS Tools. Tools from this package will work with platform. The package will uncompress into zip directory. Flash Programming Tool - Microsoft Windows* tool: Flash Programming Tool for PCH attached SPI Flash. This tool is unpacked into the /FlashProgrammingTool directory with dedicated license. ME SMBus Diagnostic Console Application. This tool is used to diagnose ME Firmware through SMBus interface. The main purpose of this tool is to provide live feedback from ME FW. ME SMBus Diagnostic Console Application is unpacked into the /MeDiagnosticConsole directory. MESDC Agent. This tool is a proxy application for MESDC. It connects MESDC using the LAN connection with the SPS FW using the HECI connection. MESDC Agent is unpacked into the /MeDiagnosticConsoleAgent directory. SPS Info tool for checking basic ME health and supported features list in /SpsInfo directory. SPS Manuf tool for validation ME functionality on the manufacturing line in /SpsManuf directory. SiEn specific Sample Update Tool source code for online update over IPMI interface in /SampleUpdateTool directory. Null HECI driver - Windows setup provides null driver removing unknown device warning from Device manager in /NullHeciDriver directory. Compliance Tests IPMI Tool Scripts in /ComplianceTestsScripts directory.

Table 2.1: Software package

No.	Package	Contents
6	SPS_Tools_4.2.61.89_epo	This is a release package with Intel SPS Tools. Tools from this package will work with platform. The package will uncompress into zip directory. ME SMBus Diagnostic Console Application. This tool is used to diagnose ME Firmware through SMBus interface. The main purpose of this tool is to provide live feedback from ME FW. ME SMBus Diagnostic Console Application is unpacked into the /MeDiagnosticConsole directory.

3. New/Changed Features

3.1. New/Changed Features

Production Version maintenance release for Purley platforms (SiEn and Full) introduces the following new features.

- New ME firmware version SPS_E5_04.00.03.235.0 is provided
- **This version of FW can be used on PRQ PCH. When running this firmware on PRQ PCH silicon, Field Programmable Fuses (FPFs) will be permanently and irreversibly set as per Intel End of Manufacturing (EOM) process flow guidelines. Please refer to Purley Manufacturing Test (IBL document 569314) for more details on the EOM process.**
- S0_RC8 mPhy table is provided

3.2. Limitations

The following list describes all the limitations for this SPS release

1. This code was tested in the following configuration:
    - Neon City RP
        - Firmware: SiEn, Full
        - PCH: LBG B0, B1, B2 also S0 and S1.
        - CPU: SKX B0, L0 and H0
        - Various memory configs: from 1 to max platform capacity RDIMMs
    - Lightning Ridge
        - Firmware: SiEn, Full
        - PCH: LBG B0 and B1
        - CPU: SKX B0 and H0
        - Various memory configs: from 1 to max platform capacity RDIMMs
    - Taliverde CRB
        - PCH: LBG B0 and B1
2. This release was tested with the following operating systems:
    - Microsoft Windows 2012 R2
    - RHEL 7.22 x64*
3. This release was tested with the following BIOS versions:
    - PLYDCRB1.86B.0140.R04.1706212120

4. To enable SMBus diagnostic interface using spsFITc:
    - PCH Strap 54 -> SMTEN = 0x1
    - Configuration -> MESDC -> SMT config -> Diagnostic/Tracing SMT Device set to SMBus
    - Configuration -> MESDC -> SMT config -> I2C Address set to 0x38
5. For executing Online Flash Update on Taliverde platform, dual image option is required:
    - DualImage value = 0x1
6. Unexpected reboots on some platforms can be avoided by changing strap:
    - PCH Strap119 -> CPUPWRGDStretchingWDTimerEnable to enabled
7. In recovery the PTT works in Failure Mode only. To exit from PTT Failure Mode, platform or host reset is required.
8. MESDC Diagnostic Console Application does not fully support Purley End Point Only mode platform.
9. Booting in recovery (via jumper) might cause missing of some PCI devices.
10. Access to RF-NVRAM memory through PECI Proxy is available only for SKX H0.
11. Prior to SPS_E5_04.00.03.137.0, ME region layout may undergo changes which affect Direct Firmware Update functionality. it is recommended to use a SPI flash programmer to perform firmware upgrade and downgrades between SPS versions.
12. Slave Attached Flash (SAF) mode does not support eSPI configurations single 20 MHz and single 30 MHz.
13. MESDC SMBus tracing when enabled may cause an exception during shutdown triggered by a ME Reset.
14. Can not Restore Factory Defaults after Online FW Update from SPS_E5_04.00.03.114.0 or to SPS_E5_04.00.03.137.0 or newer. After Online FW Upgrade FW is operational but Restore Factory Defaults ends in ME Recovery. Repair action: Please use Direct Firmware Upgrade or manual chip programming.
15. On Windows 2012R2 with Hyper-V role installed there is no possibility to change available cores number in runtime. This is OS limitation.
16. To disable global reset generated by ME during UMA Timeout, open your SPSfitc XML file and add the following lines immediately before </spsfiles>

    ```
    <fille name="SPS Special Options 1" enabled="true">

     <variable name="Option01" value="0x2FA332E6" />

    </file>
    ```

    Save the XML file and use it as input to SPSfitc to generate yor SPI chip binary file image. NOTE: this manual edit overrides the UmaTimeoutGlobalResetDelay parameter in SPSfitc GUI.
17. ME doesn't comply to requirement of maximum frame length on IPMB interface equal to 80 bytes. ME can send IPMB frames of up to 137 bytes long. OEM FW should be prepared to handle IPMB frames of up to that length.

3.3. XML Changes

Purley PLR1 RELEASE (SPS_E5_04.00.03.235.0) introduced following changes:

1. New PchStrap in "PchStrap53":
    - <PchStrap53DeepSxsupportinCSMEconfiguration value="0x0" />
2. New PchStraps in "PchStrap120":
    - <PchStrap120PNCRBDisabled value="0x0" />
    - <PchStrap120PNCRA1Disabled value="0x0" />
    - <PchStrap120PNCRA2Disabled value="0x0" />
    - <PchStrap120PNCRA3Disabled value="0x0" />
3. New PchStraps in "PchStrap133":
    - <PchStrap133SPIHostSoftwareSequencingEnableDefault value="0x1" />
4. Change PchStrap name in "PchStrap136":
    - Actual name: <PchStrap136eSPIECSlave1DeviceBusFrequency value="0x0" />, Previous name: <PchStrap136eSPIECSlave0DeviceBusFrequency value="0x0" />

3.4. Documentation Updates

Table 3.1: Current SPS Firmware Documentation.

Document Title	Revision	Ref.
SPS 4.0 External Product Specification	2.14	555192
SPS 4.0 Services Integration Guide	2.04	550581
NM 4.0 External Interface Specification	2.04	550710
SPS 4.0 ME-to-BIOS Specification	1.0.9	548530
SPS 4.0 Tools Guide	2.2	Released with the kit
SPS 4.0 Tools Guide EPO	1.1	Released with the kit
SPS 4.0 Diagnostics Guide	2.0	554904
SPS 4.0 Purley Platform Integration Guide	1.0	560168

4. Known Issues

Table 4.1: Disposition field definition.

State	Definition
Under Investigation	The sighting is being investigated.
Root Cause Identified	The root cause for the defect is identified.
Workaround Available	A temporary solution to the defect is provided until the defect is fixed.

Table 4.2: Known Issues.

Issue Id	Description
117361	**Inconsistent power consupmtion during DCMI Predictive Power Limiting**
Description	DCMI Predictive Power Limiting gives different power consumption with the same limit when set to low level (under P-States)
Root Cause	Activating Hard Power Cap policy when platform is idle may cause in excessive throttling due to wrong Hard Power Cap initialization.
Workaround	Using correction time different than 0
Status	Root cause identified
117999	**PTT intermittently stops working under some heavy load of SPS operation.**
Description	Windows TPM driver fails initializing PTT on some boots with some heavy load SPS operation
Root Cause	PTT process is starved by heavy IPMI over IPC traffic.
Workaround	None.
Status	Under Investigation.

5. Fixed Issues

Table 5.1: Disposition field definition.

State	Definition
As Designed	The issue reported is not a defect and the behavior will not be modified.
Closed no repro	The situation was not observed anymore and no further investigation is scheduled.
Fixed	Already fixed.

Table 5.2: Fixed Issues.

Issue Id	Description
118782	**Disabled Fd0V feature was setting the GPIO.**
Description	Despite fact that Fd0V was disabled the ownership of the GPIO assigned to it was always taken by the Fd0V. In case of using the same GPIO by the other feature it could not be accessed.
Root Cause	Fd0V was taking the ownership of the GPIO even when disabled.
Workaround	None
Status	Fixed.
118799	**CUPS reading is too high when running in UEFI shell on 2S config**
Description	CUPS CPU core utilization not accuracy in UEFI idle mode.
Root Cause	Code has not been tested against counter values which do not increment
Workaround	None.
Status	Fixed
118800	**HMRFPO LOCK doesn't provide valid NONCE in case of booting in recovery mode after host reset.**
Description	In recovery mode ME FW send NONCE password only on first boot of host. NONCE should be send only for first HMRFPO LOCK command but in every boot due to BIOS is not aware about NONCE between its reset.
Root Cause	In recovery mode ME FW doesn't clear flag about NONCE awareness of host resets.
Workaround	None.

Table 5.2: Fixed Issues.

Issue Id	Description
Status	Fixed.