Intel® Server Platform Services Manageability Engine Firmware for Denverton Product Line SiEn

Customer Release Notes

IPU 21.2 Beta Release for Harrisonville Platforms

Document Version 1.0

June 2021

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, withoutnotice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

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

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/#/en_US_01

Contents

List of Tables

1. Introduction

These release notes are intended for the IPU 21.2 Beta release of the Intel® Server Platform Services Manageability Engine Firmware for the Denverton SoC Product Line.

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

SPS Firmware for Harrisonville platform can be configured in SiEn SKU. 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 components included in SPS_SoC-A_04.00.04.501.0.zip package.

Subproject (component)	Location	Revision
Intel(R) SPS ME Firmware	/spsOperational.bin	SPS_SoC-A_04.00.04.501.0
Intel(R) SPS ME Recovery Boot Loader	/spsRecovery.bin	SPS_SoC-A_04.00.04.501.0
Intel(R) SPS ME Pure Recovery Boot Loader	/spsPureRecovery.bin	SPS_SoC-A_04.00.04.501.0
Intel Flash Image Tool for Server Platform Services only	/Tools/FlashImageTool	SPS_SoC-A_04.00.04.501.0
Intel® Flash Programming Tool	/Tools/FlashProgrammingTool	SPS_Tools_4.2.97.374
SPS ME SMBus Diagnostic Console	/Tools/MeDiagnosticConsole	SPS_Tools_4.2.97.374
SPS ME SMBus Diagnostic Console	/Tools/MeDiagnosticConsoleA gent	SPS_Tools_4.2.97.374
Intel® ME Info with support for SPS	/Tools/SpsInfo	SPS_Tools_4.2.97.374
SPS FW Manufacturing Tool	/Tools/SpsManuf	SPS_Tools_4.2.97.374
Sample Update Tool for SPS	/Tools/SampleUpdateTool	SPS_Tools_4.2.97.374
NULL Heci Driver	/Tools/NullHeciDriver	SPS_Tools_4.2.97.374
Compliance Tests IPMI Tool Scripts	/Tools/ComplianceTestsScripts	SPS_Tools_4.2.97.374

Table 1.2: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_SoC-A_04.00.04.501.0.zip package.

Console-Component	Revision
ME SPS Firmware Get Device Id response	50 01 04 04 02 21 57 01 00 0B 0B 00 50 10 01
ME SPS Recovery Boot Loader Get Device Id response	50 01 84 04 02 20 57 01 00 0B 0B 00 50 10 00
ME SPS Pure Recovery Boot Loader Get Device Id response	50 01 84 04 02 20 57 01 00 0B 0B 00 50 10 00
HECI MKHI_GET_FW_VERSION response	04.00.04.501
spsFITc.exe	4.0.4.501
spsFPTW64.exe, spsFPT.efi	SPS_Tools_4.2.97.374
MESDC.exe	SPS_Tools_4.2.97.374
RemoteAgentLinux64, RemoteAgentWin64.exe	SPS_Tools_4.2.97.374
spsInfoWin64.exe, spsInfoLinux64, spsInfo.efi	SPS_Tools_4.2.97.374
spsManufWin64.exe, spsManuf.efi, spsManufLinux64	SPS_Tools_4.2.97.374

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 forIPU 21.2 Beta release firmware.

Table 2.1: Software package

No.	Package	Contents
1	ReleaseNotes.pdf	This file.
2	SPS_SoC-A_04.00.04.501.0	This is a release package with Intel SPS ME Firmware and Tools for Denverton SoC platform. Uncompress the package. The package will uncompress into SPS_SoC-A_04.00.04.501.0 directory. SPSOperational - Uncompressed SPS firmwarebinary for Denverton stepping of silicon located in the main directory. SPSRecovery - Uncompressed SPS firmware binary for Denverton stepping of silicon located in the main directory. SPSPureRecovery - Uncompressed SPS firmwarebinary for Denverton stepping of silicon located in the main directory. Intel Flash Image Tool for Server Platform Services only - Microsoft 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. Flash Programming Tool - Microsoft Windows* tool: Flash Programming Tool for PCH attached SPI Flash. This tool is unpacked into the /Tools/FlashProgrammingTool directory.

Table 2.1: Software package

No.	Package	Contents
		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 /Tools/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 /Tools/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 /Tools/SpsManuf directory. SiEn specific Sample Update Tool source code for online update over IPMI interface in /Tools/SampleUpdateTool directory. Null HECI driver - Windows setup provides null driver removing unknown device warning from Device manager in /Tools/NullHeciDriver directory. Compliance Tests IPMI Tool Scripts in /Tools/ComplianceTestsScripts directory.

3. New/Changed Features

3.1. New/Changed Features

IPU 21.2 Beta Release for Harrisonville platforms introduces the following new features:

- New SPS firmware version SPS_SoC-A_04.00.04.501.0 is provided.
- **This version of FW can be used on PRQ PCH. When running this firmware on PRQ SoC silicon, Field Programmable Fuses (FPFs) will be permanently and irreversibly set as per Intel End of Manufacturing (EOM) process flow guidelines.**
- This Intel® SPS version includes functional and security updates. Users should update to the latest version.
- New PMC Patch: 4.024

3.2. Limitations

The following list describes all the limitations for this SPS release

- This code was tested in the following configuration:
  - CormorantLake, OstrichBay, Aspen Cove and Harcuvar platforms
  - Firmware SKU: SiEn
  - CPU/PCH: DNV B0, QDF: QLZH
  - SPI Flash: Winbond 25Q128FV
- This release was tested with the following operating systems:
  - Windows Server 2012 x64 R2,
  - RHEL 7.2 x64,
  - SLES 12 x64 SP1,
  - Ubuntu Server 16.04 x64,
  - Microsoft Nano Server
- This release was tested with the following BIOS versions:
  - BIOS: HAVLCRB0.X64.0016.D33.2009190650
  - mPhy tables version: RC24
  - PMC patch version: 4.024
- Features tested in this release:
  - SiEn features
- While Sca ME Power mode is set to S0/S1 and SPI frequency is equal to 17MHZ - watchdog is disabled.
- AC cycle is required after platform unlocking via orange tokens in order to bring it back to the locked state. Global reset only does not clear the debugging mode.
- The platform default power state after G3 is S0.
- When downgrading to SPS SOC-A_04.00.04.177.0 It is recommended to update the platform BIOS with the mPhy RC24 before updating SPS FW. If it is not possible, then the SPS image should be provisioned with the same mPhy version that is supported by the BIOS deployed on the platform.

- When PTT region is enabled, downgrading to SPS_SoC-A_04.00.04.177.0 or earlier, SPS FW health even A0 07 05 (manufacturing error) and A0 09 01 (firmware exception) may be observed. These are caused by ongoing security hardening changes

3.3. XML Changes

SPS_SoC-A_04.00.04.410.0 introduced following changes:

- Disable default proxy settings:
  - PeciProxyEnabled set to false,
  - PmBusProxyEnabled set to false

SPS_SoC-A_04.00.04.168.0 introduced following changes:

- Change default GPIO settings:
  - OwnershipGPIO with index from 100 to 153 with value 0
  - PadModeGPIO with index from 100 to 153 with value 0
  - PinGPIO with index from 100 to 153 with value 0x00000000000000ff
  - UsageGPIO with index from 100 to 153 with increasing value from 160 for index 100 to 213 for index 153
- Change default GPIO settings:
  - Actual value: <variable name=”PinSML1CLK” value=”0x00000000000000ff” />, previous value: ”0x0000001200000002”
  - Actual value: <variable name=”PinSML1SDA” value=”0x00000000000000ff” />, previous value: ”0x0000001100000002”
- Change value in SoCStrap 14:
  - Actualvalue:<SoCStrap14SS14bit17-ME-IntelRDirectConnectInterfaceEnabled value=”0x0” />, previous value: ”0x1”

SPS_SoC-A_04.00.04.143.0 introduced following changes:

- Change value in file ”EOM”:
  - Actual value: <variable name=”Status” value=”1” />, previous value: ”0”
- New way of SoCStraps individual naming. Please look in bellow example:
  - Actual name:<SoCStrap6**SS6bit16-**AG3EBootSelect value=”0x0” />, previous name: ”SoCStrap6AG3EBoot- Select”
- Remove SoCStraps:
  - <SoCStrap5SS5bit21-HSIOSpreadSpectrumClockingSSCDisable value=”0x0” />
  - <SoCStrap14MEROM-FirmwareROMBypassEnable value=”0x0” />
- New SoCStraps:
  - <SoCStrap7SS7bit1-BMCandBMC-lessModeSUS_SCRATCH_1bit0ErrorlogingEnable value=”0x0
  - <SoCStrap7SS7bits74-SoCBootDDRFrequency value=”0x0” />

3.4. Documentation Updates

Table 3.1: Current SPS Firmware Documentation.

Document Title	Revision	Ref.
SPS 4.0 External Product Specification	2.23	555192
SPS 4.0 Services Integration Guide	2.06	550581
NM 4.0 External Interface Specification	2.10	550710
SPS 4.0 ME-to-BIOS Specification	1.0.21	548530
SPS 4.0 Diagnostics Guide	2.0	554904
SPS 4.0 SoC Platform Integration Guide	1.1	563958

4. Fixed Issues

Table 4.1: 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 4.2: Fixed Issues.

Issue Id	Description
IPU	**2021.2 Intel Platform Update Beta**

Table 4.3: Other issues fixed since SPS_SoC-A_04.00.03.068.0

Issue Id	Description
IPU	**2021.1 Intel Platform Update**
IPU	**2020.2 Intel Platform Update**
IPU	**2020.1 Intel Platform Update**
IPU	**2019.2 Intel Platform Update**
QSR	**PSIRT-TA-201805-001, PSIRT-TA-201805-004**
Description	Intel® Converged Security Management Engine Q2'2018 Security Release
CVE-2017-5706	Mitigated security vulnerability CVE-2017-5706 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5706) details anticipated to be published Nov. 20th 2017. More details please refer to PSIRT TA 201707 002 (CDI# 574797).
CVSS v3 Score & Vectors	CVSS 8.2 High (CVSS: 3.0/AV: L/AC: L/PR: H/UI: N/S: C/C: H/I: H/A: H)
CVE-2017-5709	Mitigated security vulnerability CVE-2017-5709 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-57069) details anticipated to be published Nov. 20th 2017. More details please refer to PSIRT TA 201707 002 (CDI# 574797).
CVSS v3 Score & Vectors	CVSS 7.5 High (CVSS: 3.0/AV: L/AC: H/PR: L/UI: N/S: C/C: H/I: H/A: N)
117041	**FD0V GPIO needs to be in compliance with the LBG MGPIO Group and Pad assignment**

Description	In FITC tool the only options available for FD0 ’Group’ are ’0…255’. This is not in sync with the rest of GPIO ’Group’ assignments on LBG: ’GPP_A’, ’GPP_B’, ….
Root Cause	Tools change API for GPIO but not for all features.
Status	Fixed
Workaround	None.
117933	**SPS FITc not setting WDT Soft strap (SS4 bit0) when running in 17Mhz SPI mode.**
Description	That WDT stretching disable soft strap (SS4 bit [0]) be set to 0x1 when running in 17MHz SPI mode.
Root Cause	Design error.
Status	Fixed.
Workaround	WDT (SS4 bit [0]) could be manually set in FITc
118486	**Using bit 21 of Soft strap 5 to turn on or turn off SSC**
Description	SSC on/off feature is not visible and editable in FITc GUI.
Root Cause	Design.
Status	Fixed.
Workaround	SSC soft strap could be edited manually in XML.
118522	**IE GPIO function not work when it configure more than 20pins GPIO functions in spsfitc tool.**
Description	Configuration of more than 20 GPIO pins in spsFitc affect other GPIO function settings (IE_UART not work, IE SML bus not work), the pin onwership will be assigned to Host side.
Root Cause	Design error.
Status	Fixed.
Workaround	None.
118892	**Platforms boots in Recovery when Recovery Jumper set to None**
Description	Platform boots in Recovery, when Recovery Jumper is asserted at J4E5 and recovery Jumper pin has been set to None in spsFITc during image building .
Root Cause	Mistake in implementation.
Status	Fixed.
Workaround	None.
122540	**SML1CLK and SML1SDA are not set to None after disabling diagnostic in FITc**
Description	SML1CLK and SML1SDA should be set to ”None” if Diagnostic commands are disabled. This state of GPIO’s will change ownership from ME_MODE to HOST_MODE.
Root Cause	No linkage between GPIO and diagnostic service settings.
Status	Fixed.
Workaround	None.
123056	**End of manufacturing has wrong default value**
Description	End of Manufacturing node had wrong default value: ”EOM on HECI command”. This should be changed to ”EOM on first boot”.

Root Cause	Wrong default configuration.
Status	Fixed.
Workaround	None.
126063	**FITc - Fit crash when we click on item in search item result**
Description	FITc - Fit crash when we click on item in search item result
Root Cause	Back end issue.
Status	Fixed.
126632	**Fit Harrisonville - NVM default value for Lan Interface Selection**
Description	Lan Interface Selection in NVM tab was changed to LEK2.
Root Cause	LEK3 was not supported.
Status	Fixed.
128044	**SPS FITc tool automatically change GbE A image**
Description	When running the application in command line with parameters -gbea and -gbeb, the values are not loaded from binary GbE A.
Root Cause	Incorrect implementation.
Status	Fixed.