Intel® Server Platform Services Manageability Engine Firmware for Hewitt Lake-D SoC Product Line

Customer Release Notes

IPU 2022.1 release for Grangeville-NS Platforms

Document Version 1.0

November 2021

Contents

Table of Contents

List of Tables

1. Introduction

These release notes are intended for the Grangeville-NS of the Intel® Server Platform Services Manageability Engine Firmware for the Hewitt Lake-D SoC Product Line

The product name is abbreviated to SPS in the remainder of this document.
SPS Firmware for Grangeville platform can be configured in two different SKUs: SiEn and NM. Please refer to Intel® SPS External Product Specification [545246] for information regarding the Firmware SKU definition.

1.1. Revision Numbers of SPS Package Components

Table 1.1: Revision numbers of components of the Grangeville-NS release.

Subproject (component)	Location	Revision
Intel® SPS ME Recovery Boot Loader	SPSRecovery.bin	SPS_SoC-X_03.00.03.214.0
Intel® SPS ME Firmware	SPSOperational.bin	SPS_SoC-X_03.00.03.214.0
SPS ME Firmware configuration files	/Config/	SPS_SoC-X_03.00.03.214.0
Intel® Flash Image Tool for Server Platform Services only	/Tools/FlashImageTool/	SPS_SoC-X_03.00.03.214.0
Intel® HECI/SoL Drivers	/Tools/NullHeciDriver/	SPS_Tools_1.2.68.62
Intel® ME Info with support for SPS	/Tools/SpsInfo/	SPS_Tools_1.2.68.62
SPS FW Manufacturing Tool	/Tools/SpsManuf/	SPS_Tools_1.2.68.62
SPS ME Diagnostic Console Agent	/Tools/MeDiagnosticConsoleAgent/	SPS_Tools_1.2.68.62
SPS ME SMBus Diagnostic Console	/Tools/MeDiagnosticConsole/	SPS_Tools_1.2.68.62
Intel® Flash Programming Tool	/Tools/FlashProgrammingTool/	SPS_Tools_1.2.68.62

Table 1.2: Revision numbers visible in component properties, on the console, or over IPMI.

Console/Component	Revision
ME SPS Recovery Boot Loader Get Device Id response	00 50 01 83 03 02 20 57 01 00 06 0B 00 21 40 00
ME SPS Firmware Get Device Id response	00 50 01 03 03 02 21 57 01 00 06 0B 03 21 40 01
spsFITC.exe	3.0.3.214
spsInfo.exe, spsInfoWin.exe, spsInfoWin64.exe, spsInfo.ef, spsInfoLinux, spsInfoLinux64	1.2.68.62
spsManufWin.exe, spsManufWin64.exe and spsManuf.exe	1.2.68.62
RemoteAgentLinux, RemoteAgentLinux64, RemoteAgentWin64.exe	1.2.68.62
MESDC.exe	1.2.68.62
spsFPTW.exe, spsFPTW64.exe and spsFPT.exe	1.2.68.62
NM PTU Option ROM version File: Grangeville_SpsNMPTU_signed.rom File: Grangeville_SpsNMPTU_root.cer File: Grangeville_SpsNMPTU_signer.cer	Version 1.8 SHA- 256 hash to support UEFI Secure Boot: 5F 78 C7 AB F2 DC 38 32 90 27 01 7A 9D E7 CF AE FE 76 C9 F2 18 39 2B 60 A6 24 D0 01 45 11 CA EA

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 XP*, Microsoft Windows Vista*, Microsoft Windows 7, or DOS* 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 Grangeville-NS release firmware.

Table 2.1: Software package

No.	Package	Contents
1	ReleaseNotes	This file
2	SPS_SoC-X_03.00.03.214.0_PC-GVL_REL.zip	This is a release package with Intel® SPS ME Firmware and Tools for Hewitt Lake-D SoC UX stepping of the silicon. This package will work on Hewitt Lake-D SoC SuperSKU engineering samples and production (Hewitt Lake D) integrated chipsets as well. Uncompress the package. The package will uncompress into: SPS_SoC-X_03.00.03.214.0_PC-GVL_REL\ directory. Package contents: • Uncompressed documentation and license: PDF file in the main directory. • Uncompressed SPS firmware binaries for the Hewitt Lake-D SoC stepping of the silicon: Files SPSOperational.bin and SPSRecovery.bin in the main directory. • NM specific sample IPMI Tool scripts in /Scripts/IpmiNmScripts • Sample firmware configuration files for spsFITC in the /Config directory: BCV_SiEn.xml, BCV_NM.xml, CBM_SiEn.xml, CBM_NM.xml • 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* and DOS* tool: Flash Programming Tool for PCH attached SPI Flash. This tool is unpacked into the /Tools/FlashProgrammingTool/ directory. Note: DOS* version of the tool requires DOS4GW.exe to work. This tool is not part of the release package.

		• 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. • ME Diagnostic Console Application Agent. This tool is used to diagnose ME Firmware. ME Diagnostic Console Agent Application is unpacked into the /Tools/MeDiagnosticConsoleAgent/ directory. • SPS FW Manufacturing Tool - UEFI, Microsoft Windows and DOS tool for accessing ME Region and Flash Description Region providing additional information regarding FW status, version check and providing verifcation capabilities in /Tools/SpsManuf/. • SPS Info tool for checking basic ME health and supported features list in /Tools/SpsInfo/. • Null HECI driver - Windows setup provides null driver removing unknown device warning from Device manager in /Tools/NullHeciDriver/. • SpsNMPTU - optional component in /PTU/. This is an option ROM which can execute during BIOS POST to support the NM PTU feature. • Compliance Tests IPMI Tool Scripts in /Scripts/ComplianceTestsScripts.

3. New/Changed Features

3.1. New/Changed Features

The following list describes the new/changed functionality added in this SPS release in comparison to the former Grangeville-NS release:

- None.

3.2. Limitations

The following list describes all the limitations for this SPS release:

1. This code was tested in the following configuration:
    - Echo Canyon, Durango NS Platforms
        - Firmware: SiEn, NM
        - CPU SoC BDX-DE NS A1 (QN1C, QN1D, QN1F, QN1G)
        - BIOS Version: GNVDCRB1.86B.0091.D22.2104090334
2. This release was tested with the following operating systems:
    - MS Windows Server 2008 R2 Datacenter SP1 x64
    - MS Windows Server 2012 Datacenter x64
    - MS Windows Server 2012 R2 Datacenter x64
    - MS Windows Desktop 7 x64
    - MS Windows Desktop 8.1 x64
    - Red Hat Enterprise Linux Server 6.4 x64
    - Red Hat Enterprise Linux 6.6 x32
    - Red Hat Enterprise Linux 6.6 x64
    - Red Hat Enterprise Linux 7.1 x64
    - SUSE Linux Enterprise Server 11 SfP2 x86
    - SUSE Linux Enterprise Server 11 SP2 x64
    - SUSE Linux Enterprise Server 11 SP3 x86
    - SUSE Linux Enterprise Server 11 SP3 x64
    - SUSE Linux Enterprise Server 12 x64
    - Ubuntu Server 14 x32
    - Ubuntu Server 14 x64
    - FedoraCore 20 x32
    - FedoraCore 20 x64
    - FedoraCore 21 x32
    - FedoraCore 21 x64

- CentOS 6.6 x32
- CentOS 6.6 x64
- CentOS 7.0 x64
- ESXi 5.1
- Yocto
- KVM

3.3. Creation of SPI Flash Image

Use Flash Image Tool to assemble binary images that can be written to Flash. To see full list of options supported by FIT use command:

```
Tools\FlashImageTool\FITc.exe /?
```

To build only the ME region image with SPS firmware in dual-image configuration, and without Flash descriptor, BIOS and GbE regions use the following command:

```
Tools\FlashImageTool\FITc.exe /b /flashcount 0 <xml-file-path>
```

Note: this image is not complete SPI Flash image, but just ME region.

The <xml-file-path> should be replaced with a path to the proper XML configuration file. The sample configuration files included in the release package are:

- BCV_NM.xml Dual image configuration for Datacenter Manager Firmware (NM) on Beverly Cove platform.
- CBM_SiEn.xml Dual image configuration for Datacenter Manager Firmware (SiEn) on Camelback Mountain platform.
- BCV_SiEn.xml Dual image configuration for Datacenter Manager Firmware (SiEn) on Beverly Cove platform.
- CBM_NM.xml Dual image configuration for Datacenter Manager Firmware (NM) on Camelback Mountain platform.

To build a complete SPI Flash image with Flash descriptor region and SPS firmware in dual-image configuration use the following command:

```
Tools\FlashImageTool\FITc.exe /b <xml-file-path>
```

To build a complete SPI Flash image with Flash descriptor, BIOS, GbE and SPS firmware in dual-image configuration use the following command:

```
Tools\FlashImageTool\FITc.exe /b /bios <bios-file> /gbe <GbE-file> <xml-file-path>
```

Note: the default Flash size is 128 Mbits (16 MB).

To force building single image configuration use either a FIT command line option '/SingleImage' or the change can be done and saved in XML by omitting the option '/b' in the FIT command line to allow opening GUI window and in the GUI right-click on Layout -> ME Region -> "OPR2" Partition and select 'Disable' to disable this secondary code partition.

Note: if '/b' switch is not used, FIT GUI will be presented and adjustments to the default XML can be made and saved.

Note: FIT uses FITc.ini to set CurWorkDir, WorkingDir and SourceDir, so FIT batch file usage assumes appropriate working/source directories setting (pushd/popd can be used).

Warning: ME must have the Flash erase sector size set. The provided XML files are preconfigured for 4kB sectors. If one is going to use 64kB sectors it must be set in ME parameters. Run FIT in GUI mode by omitting '/b' option in command line, double click on Layout -> ME Region -> Configuration Block Erase Size and set the desired sector size. When done save the new settings with 'Ctrl-S' and if needed build the Flash image with 'F5'.

3.4. Documentation Updates

Table 3.1: Current SPS Firmware Documentation.

Document Title	Revision	Ref.
SPS 3.0 External Product Specification	1.0	545246
SPS 3.0 Services Integration Guide	1.0	554953
Intel® Intelligent Power Node Manager 3.0 External Interface Specification using IPMI	1.0.7	513973
Intel® Server Platform Services (Intel® SPS) 3.0 Firmware ME-BIOS Interface Specification	1.0	545932
Grangeville Platform Design Guide	1.0	543448
SPS Firmware Bringup Guide	Included in each FW release	

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.
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: Known Issues.

Issue Id	Description

5. Fixed Issues

Table 5.1: Fixed Issues in previous releases

Issue Id	Description
CCG0100859813	Adjust diagnostic commands filtering across different interfaces
Problem	Some of not allowed MESDC commands per-intefrace were unblocked
Implication	Security issue.
Note	
Image	Operational, Recovery
Root Cause	Implementation
Workaround	None
Status	Fixed
CCG0100856998	The internal error of ME-FW occurred during POST after reboot from Windows Server with Hyper-V
Problem	The health event is generated due to a ME watchdog timeout
Implication	Sporadically NM health event in the system log is observed after reboot from OS.
Note	
Image	Operational
Root Cause	VDM response timeout procedure didn't notify IBPECI thread to drop current transaction. Hence the IBPECI thread self-triggered and caused WDG timer to expire.
Workaround	None
Status	Fixed
CCG0100859661	SOC package pwr sometimes report 0 Watt issue
Problem	Extremely sporadically a VCU response to the PCH temperature update may be mistakenly treated by ME as a response to some other IBPECI request.
Implication	Data-mismatch
Note	
Image	Operational
Root Cause	VDM flag resetting mechanism causes (extreme sporadic) IBPECI ping-pong de-synchronization and hence data-mismatch.
Workaround	None
Status	Fixed
CCG0100859702	Exception in Susram after sending Diagnostic command SendRawPmBusReq

Problem	DiagnosticsValTestsHandlerFunPMBusTransport command blocks sending any data
Implication	Security issue.
Note	
Image	Operational
Root Cause	Function which handles diagnostic command SendRawPmbus is broken
Workaround	None
Status	Fixed
CCG0100859712	Exception in Susram after loop of Diagnostic command
Problem	FlashPerfTestEraseStartReq diagnostic command was unblocked on diagnostic interface
Implication	Security issue.
Note	
Image	Operational
Root Cause	FlashPerfTestEraseStartReq diagnostic command was unblocked on all interfaces
Workaround	None
Status	Fixed
CCG0100859663	ME sends IBPECI transactions after IBPECI timeout
Problem	Unexpected Grangeville specific IBPECI traffic in case of a timeout condition
Implication	The PCH temperature updates are still being sent
Note	
Image	Operational
Root Cause	When ApiBlocked flag was set, then Grangeville specific WritePchTemp IBPECI transactions weren't blocked.
Workaround	None
Status	Fixed
CCG0100859288	Diagnostic interface crash after sending IPMI command SendRawPmBusReq
Problem	Sending Send Raw Pmbus IPMI command without payload causes crash of diagnostic interface.
Implication	Diagnostic interface is not responding.
Note	
Image	Operational
Root Cause	SMT hardware not allowed I2c transaction write length = 0 when transport protocol is I2C and transaction type = Write

Workaround	None
Status	Fixed
CCG0100859245	GetSensorValue command returns zero readings from 0xAC, 0xAF, 0xBB sensors
Problem	Platform power, derated power and power efficiency sensors respond with compilation code 0x8D and zero values
Implication	Autoconfiguration functionality could not be used
Note	
Image	Operational
Root Cause	32bit variable was being passed to function which accepts 8bit variable
Workaround	None
Status	Fixed
CCG0100859104	Missing power reading Policy not activating
Problem	Missing power reading policy is not activating. Throttling statistics are equal 0%. No power draw reduction detected.
Implication	Platform is not throttled after missing power reading timeout is detected
Note	
Image	Operational
Root Cause	Wrong comparison condition
Workaround	None
Status	Fixed
CCG0100853846	Region Order setting in XML does not work
Problem	Region Order was not allowing to put a mini OS in the image
Implication	Cannot run the OS image from SPI flash device on CS1
Note	
Image	Operational, Recovery
Root Cause	Design
Workaround	None
Status	Fixed
CCG0100850589	AAh completion returned in response for “Get CPU And Memory Temperature” command.
Problem	Sometimes SPS ME FW may response with AAh completion code on 4Bh “Get CPU And Memory Temperature” command after thermal trip test.
Implication	Unable to read CPU and MEM temperature after shutdown caused by thermal trip.
Note	
Image	Operational

Root Cause	Invalid error handling in case PECI Wire interface failure.
Workaround	None
Status	Fixed
CCG0100851095	Node Busy response for IPMI commands.
Problem	Sometimes SPS ME FW response with C0h “Node busy” completion code on IPMI commands.
Implication	IPMI communication impacted.
Note	
Image	Operational
Root Cause	Components synchronization issue.
Workaround	None
Status	Fixed
CCG0100202534	“Get NM PTU Statistics” IPMI command returns too many bytes.
Problem	“Get NM PTU Statistics” IPMI command returns too many bytes. Responses contain 62 bytes instead of expected 60 bytes.
Implication	External tools may be affected.
Note	
Image	Operational
Root Cause	Codding error.
Workaround	None
Status	Fixed
CCG0100850168	Minimal configuration functionality did not set appropriate bit.
Problem	Minimal configuration functionality did not set appropriate bit. Bit 7 of HECI-1 GS_SHDW Register was set instead of bit 8 of HECI-1 GS_SHDW Register.
Implication	Functionality lays on Minimal configuration will be misled.
Note	
Image	Operational
Root Cause	Codding error.
Workaround	None
Status	Fixed
CCG0100202521	CPU stuck at Pn/Pm after NM PTU characterization.
Problem	NM PTU Characterization CPU stuck at Pn/Pm after CPU Min Power characterization.
Implication	Platform may be throttled.
Note	

Image	Operational
Root Cause	Too strict data validation in inner function.
Workaround	None
Status	Fixed
CCG0100849947	Set Turbo Synchronization Ratio doesn't apply.
Problem	Sometimes “Set Turbo Synchronization Ratio” IPMI command doesn’t change actual Turbo Synchronization Ratio value.
Implication	Turbo Synchronization Ratio could not be changed.
Note	
Image	Operational
Root Cause	Too strict data validation in inner function.
Workaround	None
Status	Fixed
CCG0100804339	0W in HW Protection domain statistics
Problem	Sometimes power consumption statistics for HW Protection domain are 0.
Implication	HW Protection functionality couldn’t be used.
Note	
Image	Operational
Root Cause	Wrong readings source taken by HW protection domain.
Workaround	None
Status	Fixed
CCG0100849541	ME enter recovery mode when set altitude -1000 or 10000.
Problem	When altitude set to -1000 or 10000 ME unexpectedly enter recovery mode.
Implication	ME stay in Recovery mode.
Note	
Image	Operational
Root Cause	Wrong comparison condition.
Workaround	None
Status	Fixed
CCG0100845948	Default ICC register values are not correct
Problem	Value of ICC registers is not met requirements.
Implication	Value of ICC registers is not met requirements.
Note	
Image	Operational

Root Cause	Wrong data taken.
Workaround	None
Status	Fixed
CCG0100231731	Recovering from hibernate or sleep launches PTU
Problem	PTU launches when coming out of hibernate and sleep states
Implication	PTU should only launch coming out of S5 so this launch is undesirable
Note	Not ME defect. BIOS issue.
Image	Operational
Root Cause	Extra reset from BIOS without event notification
Workaround	Do not activate Sleep or Hibernate
Status	Fixed
CCG0100202254	PTU option ROM not running at Max performance
Problem	Platform does not run at max performance
Implication	When characterizing max, the power draw may or may not reach TDP
Note	Not a defect
Image	Operational
Root Cause	Unknown
Workaround	None
Status	Fixed
CCG0100844240	ME is intermittently and randomly going into Recovery Mode
Problem	ME is intermittently and randomly going into Recovery Mode.
Implication	ME stay in Recovery mode.
Note	
Image	Operational
Root Cause	Wrong Segment Defined Feature configuration validation.
Workaround	None
Status	Fixed
CCG0100846153	Unexpected Completion Code during creating boot time policy.
Problem	Node Manager returns completion code 0xff for creating boot time policy during DC OFF state.
Implication	Unable to create boot time policy during DC OFF state.
Note	
Image	Operational
Root Cause	Side effects of other changes

Workaround	None
Status	Fixed
CCG0100846154	Boot time policy issue.
Problem	Boot mode policy doesn't write cores disabled setting to HECI-2 HFS register
Implication	Boot mode policy not properly operating.
Note	
Image	Operational
Root Cause	Side effects of other changes
Workaround	None
Status	Fixed
CCG0100790075	P/T states incorrect values are returned
Problem	Wrong value returned from Get Max Allowed CPU P-states/T-states while limiting using Total Power Budget
Implication	Wrong value returned from Get Max Allowed CPU P-states/T-states while limiting using Total Power Budget
Note	Issue fixed in microcode version 0xb
Image	Operational
Root Cause	Incorrect BDX-DE CPU fusing
Workaround	None
Status	Fixed
CCG0100859907	CLKOUT_PEGA / CLKOUT_PEGB default option/mask need to fit BDX-DE architecture
Problem	CLKOUT_PEGA and CLKOUT_PEGB are both hidden in the mask but enabled as default
Implication	Not ME defect, tool issue
Note	
Image	Operational, Recovery
Root Cause	Mismatch with BDX-DE CPU architecture
Workaround	None
Status	Fixed
CCG0100859939	spsFITc - increase PDR region MAX length
Problem	Cannot build image with PDR region larger than 0x00500000
Implication	Not ME defect, tool issue
Note	
Image	Not related
Root Cause	Implementation

Workaround	None
Status	Fixed
CCG0100860057	Memory Thermal Throttling seen without active policy on production Grangeville systems
Problem	Memory Thermal Throttling seen without active policy
Implication	Memory Thermal Throttling seen without active policy
Note	
Image	Operational
Root Cause	Before starting the load, Get NM Capabilities reports min/max values as configured by BIOS: 0-3 Watts. When workload is running, however, DIMMs consume ~5Watts, and max power reported by Get NM Capabilities is increased to reflect that. Due to an improper implementation, after adjusting capabilities for memory domain, misinterprets new max memory power draw value (~4.5W) as new control signal, and configures memory RAPL limits.
Workaround	None
Status	Fixed

Table 5.2: Fixed Issues

Issue Id	Description