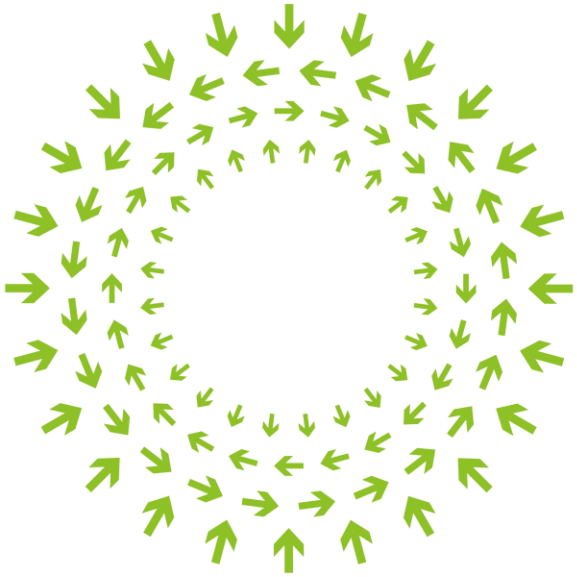


OPEN

Compute Project

Inspur Rack Management Controller Module Design Specification

Mine Hill

Rev 1.3.1

Author: Inspur Mine Hill Team

Table of Contents

1. LICENSE 3

2. SCOPE 4

3. CONTENT. 5

3.1 Overview 5

3.2 Product Overview 5

3.3 Product standard 5

4. PHYSICAL SPECIFICATIONS 5

4.1 Block Diagram Reference for Base Specification 6

4.2 SMBus Manager Topology 7

4.3 Placement and Form Factor 7

4.4 Management ASIC 8

4.5 PCB Stack-Up 9

4.6 PCIe Pin Definition 9

4.7 VSC7434 Switch Port Mapping 10

4.8 Motherboard Power System 12

4.9 Hot-Swap Controller (HSC) Circuit 12

5. ENVIRONMENTAL AND REGULATIONS 12

5.1 Controller high altitude 12

5.2 Controller relative humidity 13

5.3 Controller Temperature 13

Appendix 13

1. License

Open Web Foundation Contributor License Agreement (CLA 1.0)

The Purpose of this Contributor License Agreement. This CLA sets forth the terms under which I will participate in and contribute to the development of the Specification. Capitalized terms are defined in the CLA's last section.

Identify the Specification here:
OpenRMC Module Hardware Specification

List any requirements and objectives for the Specification:
The objective of this document is to specify the requirements for hardware component of a rack manager controller contribution, specifically the specification of the RMC hardware module.

The scope of the Specification shall be limited to the following:
The scope of the specification is limited to the hardware component of a rack manager controller (RMC) platform, which the firmware resides for the OpenRMC solution.

Without limiting the scope, the following subject matter is specifically out of scope under this Specification:
The specification doesn't specify any of the firmware aspect of the rack manager controller.

Notwithstanding the foregoing, the Scope shall not include (a) any enabling technologies that may be necessary to make or use any product or portion thereof that complies with a Specification, but are not themselves expressly set forth in a Specification (e.g., semiconductor manufacturing technology, semiconductor packaging technology, processor architecture/microarchitecture, processor instruction sets, compiler technology, etc.); or (b) the implementation or use of other specifications published and made available by any other standards body, but referred to in the body of a Specification and not first developed in the OCP, even if required for compliance with a
Specification; or (c) any portions of any product and any combinations thereof the purpose or function of which is not required for compliance with a Specification; or (d) reference or informational portions of a Specification.

If signing this CLA as a Bound Entity:
Signed Name: Wilson Guo
Email Address: guohongchang@inspur.com
Date: Aug. 21st, 2020
Bound Entity: Inspur Electronic Information Industry Co. Ltd

2. Scope

This standard provides the reference board-specific information detailing the features and functionality of a general management controller card for adoption by the Open Compute Project community. The purpose of this document is to define management controller card that is capable of deployment within scaled out data centers as well as the other rack components with manageable firmware functionality enabled. In the creation of the Mine Hill specification, considerations are made for management controller cards that were in production at time of specification release that would fulfill these needs.

This document is not intended to be used solely as a basis for a procurement of OCP compatible products. The OCP community may have additional requirements. These incremental requirements can be captured in additional procurement documentation.

3. Content.

3.1 Overview

Mine Hill is PCIe Gen3 x16 Riser card, based on manageable Aspeed 2400 BMC chip. The management controller accommodates Dual Ethernet port and legacy RS232 COM port as well. Mine Hill is designed in the Q2 of 2016.

3.2 Product Overview

Mine Hill is a completely independent research and development of value-add management modular adapter. Based on Aspeed® 2400 chip, support two 10/100/1000Mb Ethernet port for out-of-band management capability. PCI Express support expansion slot X16.

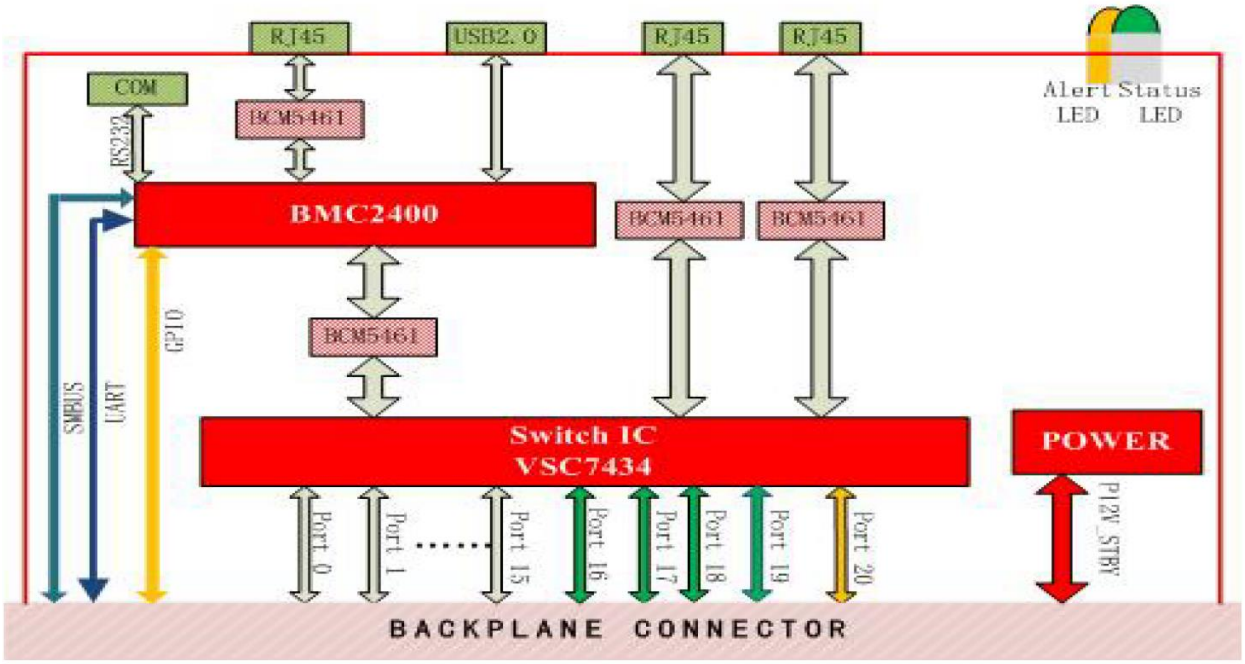
3.3 Product standard

(*BOLD & Underline is MUST HAVE for Mine Hill*)

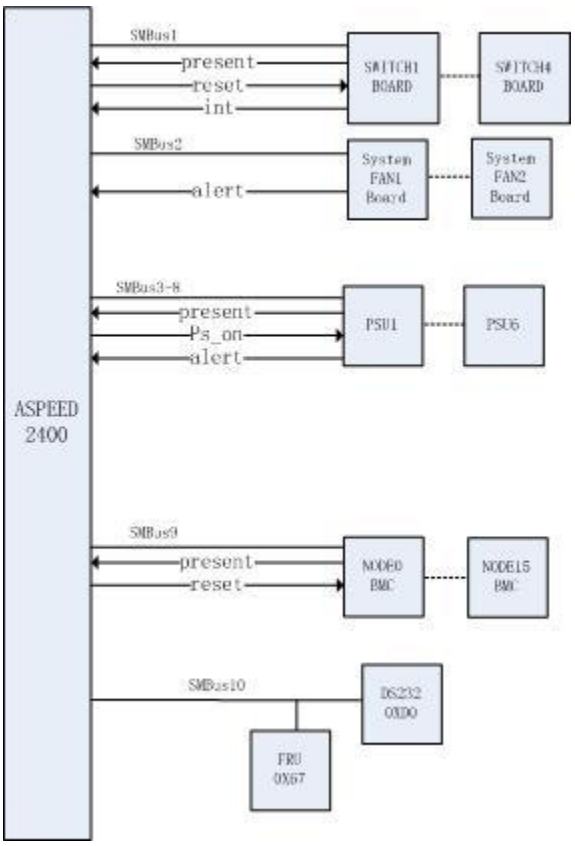
Specification	Description
Architecture	***PCIe based Health and Remote management ASIC***
Processor	***Aspeed 2400 BMC Chip***
Upgradeability	***Firmware upgradeable via Flash ROM***
Interfaces	● ***OOB Network connection (10/100/1000Mb/s) on board*** ● ***OOB Network connection (10/100/1000Mb/s) on board*** ● ***Dual USB ports*** ● ***RS232 COM Port***

4. Physical Specifications

4.1 Block Diagram Reference for Base Specification

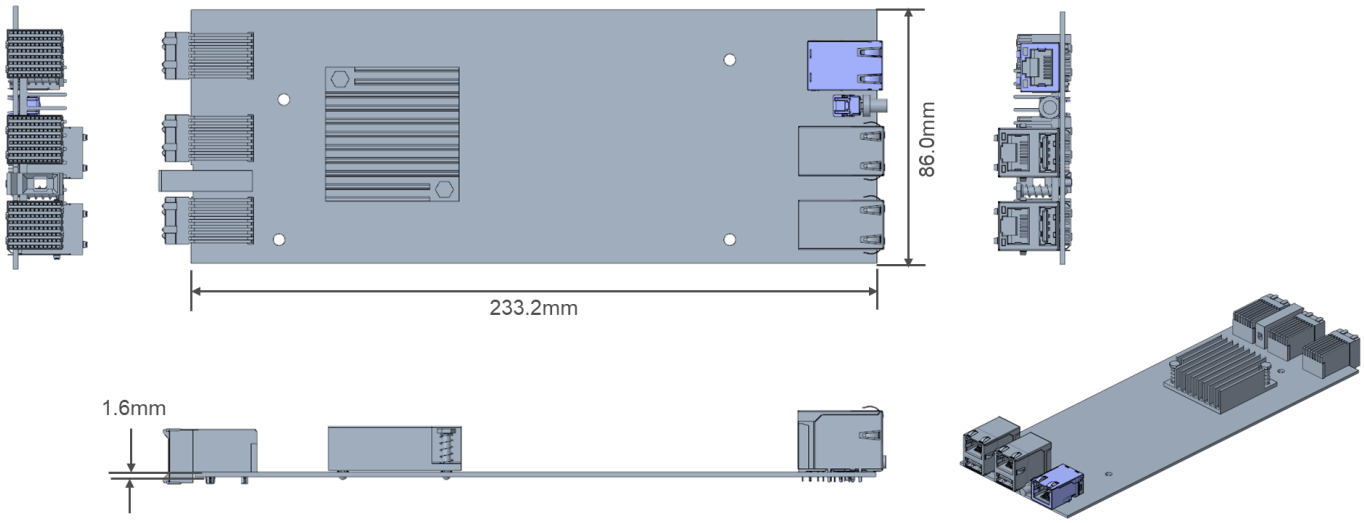


4.2 SMBus Manager Topology



4.3 Placement and Form Factor

Mine Hill board form factor is within the square limitation of 3.39 inch by 9.18 inch (3.39”x9.18”) or 86mm by 233.2mm (86mm x 233.2mm).
And Figure 4-2 illustrates a ***reference of board overview.*** The placement is meant to show key components ’relative positions, while exact dimension and position information would be exchanged by DXF format for layout and 3D model for mechanical, and ***as long as the board remain within the 3.39” x 9.18” with the Power Supply location both on the right hand side; that any alternative OxM design of the board shall able to claim as meeting the Mine Hill specification.***



4.4 Management ASIC

The management controller is an independent system of host system. This independent system has its own processor and memory; The host system can be managed by this BMC system even if host hardware or OS hang or went down. This controller integrates Aspeed AST2400 and Broadcom BCM5461 ASICs.

4.4.1 BMC AST2400

Aspeed AST2400 baseboard management controller is the center of the management controller. This device provides support for many platform functions including system video capabilities, legacy Super I/O functions, hardware monitoring functions, and incorporates an ARM1176JZF-S 32-bit RISC CPU microcontroller to host an IPMI 2.0 compliant managemnt firware stack.

- AST2400 Advanced PCIe Graphics & Remote Management Processor:
- Baseboard Management Controller
- 2D Video Graphic Adapter with PCIe Bus Interface
- Native PCIe support
- Flash Memory NOR/NAND/SPI flash memory
- ARM9@400MHz

4.4.2 Broadcom BCM5461

Triple-speed 1000BASE-T/100BASE-TX/10BASE-T Energy Efficient Ethernet (IEEE 802.3az) Gigabit (GbE) transceiver integrated into a single monolithic CMOS chip.

- Single-chip integrated triple-speed Energy Efficient Ethernet Gigabit transceiver. Support for the following copper line interfaces: 1000BASE-T IEEE 802.3ab, 100BASE-TX IEEE 802.3u and 10BASE-T IEEE 802.3
- Supports RGMII MAC interface
- IEEE 802.3az-compliant support — Support for native EEE MACS — support for Not Recommended for New Design non-EEE MACs using AutogrEEEn® mode

4.5 PCB Stack-Up

PCB Stack-up					Single End(mil)		Differential Pair(mil)				Differential Pair(mil)				Reference
Layer	Material:	IT180-A		Thickness	55Ω	55Ω	90Ω		90Ω		100Ω		100Ω		
					Customer	PCB Vendo	Customer		PCB Vendor		Customer		PCB Vendor		
		Glass Type		unit : mil	W	W	W	S	W	S	W	S	W	S	
	Solder mask	Green Liquid		0.6											
TOP	SIGNAL	Copper	0.333oz+plating	1.6	4.5	4.8	5.7	7.4	5.9	7.2	4.4	8.7	4.8	8.3	L2
		p.p	106*2	3.85											
L2	GND	Copper	1oz	1.2											
		core	0.15mm	5.91											
L3	SIGNAL	Copper	1oz	1.2	5	5	6.5	7.8	6.3	8	4.8	9.5	4.9	9.4	L2 & L4
		p,p	2116*3	12.96											
L4	GND	Copper	1oz	1.2											
		core	0.11mm	4.33											
L5	PWR	Copper	1 oz	1.2											
		p,p	2116*3	12.96											
L6	SIGNAL	Copper	1oz	1.2	5	5	6.5	7.8	6.3	8	4.8	9.5	4.9	9.4	L5& L7
		core	0.15mm	5.91											
L7	GND	Copper	1oz	1.2											
		p.p	106*2	3.85											
BOT	SIGNAL	Copper	0.333oz+plating	1.60	4.5	4.8	5.7	7.4	5.9	7.2	4.4	8.7	4.8	8.3	L17
	Solder mask	Green Liquid		0.6											
		Total thickness:	1.6mm												
		Specification:	1.6mm												

4.6 PCIe Pin Definition

Connector A					Connector B					Connector C			
Signal	pin	pin	Signal		Signal	pin	pin	Signal		Signal	pin	pin	Signal
SMGII7_TXP	A1	B2	SGMII6_TXP		SGMII5_TXP	A1	B2	SGMII14_TXP		N1_SMC1_GPIO1_Q	A1	B2	N1_SMC1_GPIO2_Q
SGMII7_TXN	B1	C2	SGMII6_TXN		SGMII5_TXN	B1	C2	SGMII14_TXN		N2_SMC1_GPIO1_Q	B1	C2	N2_SMC1_GPIO2_Q
SGMII7_RXP	D1	E2	SGMII6_RXP		SGMII5_RXP	D1	E2	SGMII14_RXP		N3_SMC1_GPIO1_Q	D1	E2	N3_SMC1_GPIO2_Q
SGMII7_RXN	E1	F2	SGMII6_RXN		SGMII5_RXN	E1	F2	SGMII14_RXN		N4_SMC1_GPIO1_Q	E1	F2	N4_SMC1_GPIO2_Q
PSU1_SCL3	G1	H2	PSU2_SCL4		NODE1_PRESENT_N	G1	H2	NODE2_PRESENT_N		N5_SMC1_GPIO1_Q	G1	H2	N5_SMC1_GPIO2_Q
PSU1_SDA3	H1	I2	PSU2_SDA4		NODE3_PRESENT_N	H1	I2	NODE4_PRESENT_N		N6_SMC1_GPIO1_Q	H1	I2	N6_SMC1_GPIO2_Q
PSU3_SCL5	J1	K2	PSU4_SCL6		NODE5_PRESENT_N	J1	K2	NODE6_PRESENT_N		N7_SMC1_GPIO1_Q	J1	K2	N7_SMC1_GPIO2_Q
PSU3_SDA5	K1	L2	PSU4_SDA6		NODE7_PRESENT_N	K1	L2	NODE8_PRESENT_N		N8_SMC1_GPIO1_Q	K1	L2	N8_SMC1_GPIO2_Q
SGMII5_TXP	A3	B4	SGMII4_TXP		SGMII3_TXP	A3	B4	SGMII12_TXP		N9_SMC1_GPIO1_Q	A3	B4	N9_SMC1_GPIO2_Q
SGMII5_TXN	B3	C4	SGMII4_TXN		SGMII3_TXN	B3	C4	SGMII12_TXN		N10_SMC1_GPIO1_Q	B3	C4	N10_SMC1_GPIO2_Q
SGMII5_RXP	D3	E4	SGMII4_RXP		SGMII3_RXP	D3	E4	SGMII12_RXP		N11_SMC1_GPIO1_Q	D3	E4	N11_SMC1_GPIO2_Q
SGMII5_RXN	E3	F4	SGMII4_RXN		SGMII3_RXN	E3	F4	SGMII12_RXN		N12_SMC1_GPIO1_Q	E3	F4	N12_SMC1_GPIO2_Q
PSU5_SCL7	G3	H4	PSU6_SCL8		NODE9_PRESENT_N	G3	H4	NODE10_PRESENT_N		N13_SMC1_GPIO1_Q	G3	H4	N13_SMC1_GPIO2_Q
PSU5_SDA7	H3	I4	PSU6_SDA8		NODE11_PRESENT_N	H3	I4	NODE12_PRESENT_N		N14_SMC1_GPIO1_Q	H3	I4	N14_SMC1_GPIO2_Q
SWITCH_SCL1	J3	K4	SW3_PRESENT_N		NODE13_PRESENT_N	J3	K4	NODE14_PRESENT_N		N15_SMC1_GPIO1_Q	J3	K4	N15_SMC1_GPIO2_Q
SWITCH_SDA1	K3	L4	SW4_PRESENT_N		NODE15_PRESENT_N	K3	L4	NODE16_PRESENT_N		N16_SMC1_GPIO1_Q	K3	L4	N16_SMC1_GPIO2_Q
SGMII3_TXP	A5	B6	SGMII2_TXP		SGMII11_TXP	A5	B6	SGMII10_TXP		SGMII19_TXP	A5	B6	SGMII18_TXP
SGMII3_TXN	B5	C6	SGMII2_TXN		SGMII11_TXN	B5	C6	SGMII10_TXN		SGMII19_TXN	B5	C6	SGMII18_TXN
SGMII3_RXP	D5	E6	SGMII2_RXP		SGMII11_RXP	D5	E6	SGMII10_RXP		SGMII19_RXP	D5	E6	SGMII18_RXP
SGMII3_RXN	E5	F6	SGMII2_RXN		SGMII11_RXN	E5	F6	SGMII10_RXN		SGMII19_RXN	E5	F6	SGMII18_RXN
FAN_SCL2	G5	H6	PSU1_PWRON_N		PSU1_PRST_N	G5	H6	P12V_STBY		SW3_INT1_N	G5	H6	SW4_INT1_N
FAN_SDA2	H5	I6	PSU2_PWRON_N		PSU2_PRST_N	H5	I6	P12V_STBY		PSU3_ALERT_N	H5	I6	FAN1_ALERT_N
NODE_SCL9	J5	K6	PSU3_PWRON_N		PSU3_PRST_N	J5	K6	P12V_STBY		PSU4_ALERT_N	J5	K6	FAN2_ALERT_N
NODE_SDA9	K5	L6	PSU4_PWRON_N		PSU4_PRST_N	K5	L6	P12V_STBY		SW3_RESET_N	K5	L6	SW4_RESET_N
SGMII1_TXP	A7	B8	SGMII0_TXP		SGMII9_TXP	A7	B8	SGMII8_TXP		SGMII17_TXP	A7	B8	SGMII16_TXP
SGMII1_TXN	B7	C8	SGMII0_TXN		SGMII9_TXN	B7	C8	SGMII8_TXN		SGMII17_TXN	B7	C8	SGMII16_TXN
SGMII1_RXP	D7	E8	SGMII0_RXP		SGMII9_RXP	D7	E8	SGMII8_RXP		SGMII17_RXP	D7	E8	SGMII16_RXP
SGMII1_RXN	E7	F8	SGMII0_RXN		SGMII9_RXN	E7	F8	SGMII8_RXN		SGMII17_RXN	E7	F8	SGMII16_RXN
SMC_UART_TX	G7	H8	PSU5_PWRON_N		PSU5_PRST_N	G7	H8	P12V_STBY		SW1_INT1_N	G7	H8	SW2_INT1_N
SMC_UART_RX	H7	I8	PSU6_PWRON_N		PSU6_PRST_N	H7	I8	P12V_STBY		PSU1_ALERT_N	H7	I8	PSU5_ALERT_N
SW1_PRESENT_N	J7	K8	NODE_SCL11		NODE_SMC1_INT_N	J7	K8	P12V_STBY		PSU2_ALERT_N	J7	K8	PSU6_ALERT_N
SW2_PRESENT_N	K7	L8	NODE_SDA11		SMC_ID	K7	L8	SW_BMC_SEL_N		SW1_RESET_N	K7	L8	SW2_RESET_N
GND	A2	G2	GND		GND	A2	G2	GND		GND	A2	G2	GND
GND	A4	G4	GND		GND	A4	G4	GND		GND	A4	G4	GND
GND	A6	G6	GND		GND	A6	G6	GND		GND	A6	G6	GND
GND	A8	G8	GND		GND	A8	G8	GND		GND	A8	G8	GND
GND	C1	I1	GND		GND	C1	I1	GND		GND	C1	I1	GND
GND	C3	I3	GND		GND	C3	I3	GND		GND	C3	I3	GND
GND	C5	I5	GND		GND	C5	I5	GND		GND	C5	I5	GND
GND	C7	I7	GND		GND	C7	I7	GND		GND	C7	I7	GND
GND	D2	J2	GND		GND	D2	J2	GND		GND	D2	J2	GND
GND	D4	J4	GND		GND	D4	J4	GND		GND	D4	J4	GND
GND	D6	J6	GND		GND	D6	J6	GND		GND	D6	J6	GND
GND	D8	J8	GND		GND	D8	J8	GND		GND	D8	J8	GND
GND	F1	L1	GND		GND	F1	L1	GND		GND	F1	L1	GND
GND	F3	L3	GND		GND	F3	L3	GND		GND	F3	L3	GND
GND	F5	L5	GND		GND	F5	L5	GND		GND	F5	L5	GND
GND	F7	L7	GND		GND	F7	L7	GND		GND	F7	L7	GND

4.7 VSC7434 Switch Port Mapping

Port Number	Port Names	Pin Names		CONN
0	DEV1G 0	SGMII0_RXP SGMII0_RXN	SGMII0_TXP SGMII0_TXN	J2
1	DEV1G 1	SGMII1_RXP SGMII1_RXN	SGMII1_TXP SGMII1_TXN	J2
2	DEV1G 2	SGMII2_RXP SGMII2_RXN	SGMII2_TXP SGMII2_TXN	J2
3	DEV1G 3	SGMII3_RXP SGMII3_RXN	SGMII3_TXP SGMII3_TXN	J2
4	DEV1G 4	SGMII4_RXP SGMII4_RXN	SGMII4_TXP SGMII4_TXN	J2
5	DEV1G 5	SGMII5_RXP SGMII5_RXN	SGMII5_TXP SGMII5_TXN	J2
6	DEV1G 6	SGMII6_RXP SGMII6_RXN	SGMII6_TXP SGMII6_TXN	J2
7	DEV1G 7	SGMII7_RXP SGMII7_RXN	SGMII7_TXP SGMII7_TXN	J2
8	DEV1G 8	SGMII8_RXP SGMII8_RXN	SGMII8_TXP SGMII8_TXN	J3
9	DEV1G 9	SGMII9_RXP SGMII9_RXN	SGMII9_TXP SGMII9_TXN	J3
10	DEV1G 10	SGMII10_RXP SGMII10_RXN	SGMII10_TXP SGMII10_TXN	J3
11	DEV1G 11	SGMII11_RXP SGMII11_RXN	SGMII11_TXP SGMII11_TXN	J3
12	DEV1G 12	SGMII12_RXP SGMII12_RXN	SGMII12_TXP SGMII12_TXN	J3
13	DEV1G 13	SGMII13_RXP SGMII13_RXN	SGMII13_TXP SGMII13_TXN	J3
14	DEV1G 14	SGMII14_RXP SGMII14_RXN	SGMII14_TXP SGMII14_TXN	J3
15	DEV1G 15	SGMII15_RXP SGMII15_RXN	SGMII15_TXP SGMII15_TXN	J3
16	DEV1G 16	SGMII16_RXP SGMII16_RXN	SGMII16_TXP SGMII16_TXN	J11
17	DEV1G 17	SGMII17_RXP SGMII17_RXN	SGMII17_TXP SGMII17_TXN	J11
18	DEV1G 18	SGMII18_RXP SGMII18_RXN	SGMII18_TXP SGMII18_TXN	J11
19	DEV1G 19	SGMII19_RXP SGMII19_RXN	SGMII19_TXP SGMII19_TXN	J11
20	DEV1G 20	SGMII20_RXP SGMII20_RXN	SGMII20_TXP SGMII20_TXN	NA
21	DEV1G 21	SGMII21_RXP SGMII21_RXN	SGMII21_TXP SGMII21_TXN	BCM5461SA3KFBG
22	DEV1G 22	SGMII22_RXP SGMII22_RXN	SGMII22_TXP SGMII22_TXN	BCM5461SA3KFBG
23	DEV1G 23	SGMII23_RXP SGMII23_RXN	SGMII23_TXP SGMII23_TXN	BCM5461SA3KFBG

4.8 Motherboard Power System

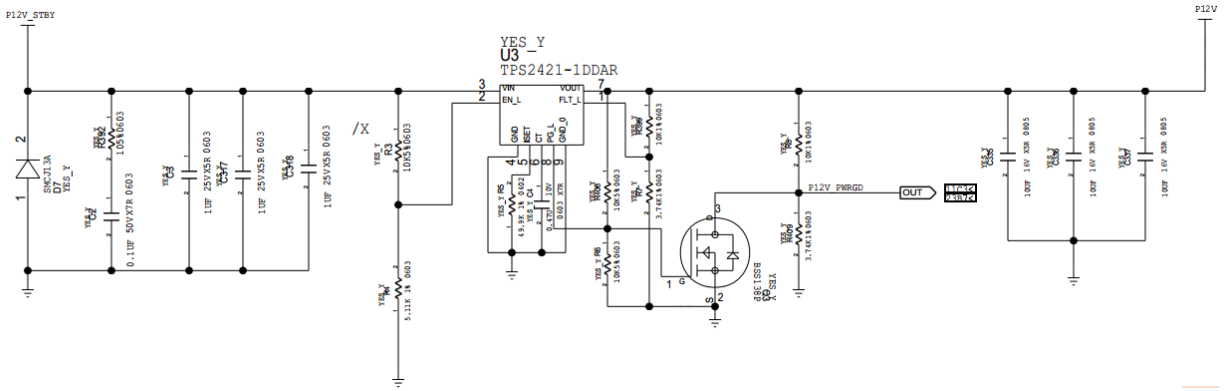
4.8.1 Input Voltage

DC Input Voltage Range: +11.8V to +12.6V DC

DC Input Nominal Voltage: +12.2V

4.9 Hot-Swap Controller (HSC) Circuit

Hot plug and hot swap support is optional for CMC card implementers. These events need to be carefully orchestrated with the operating system and system management entity to prevent a system hang. A surprise extraction may occur in some instances when resources have not been quiesced and the card is removed. Many aspects of the system are involved in processing such an event in both cases. The current scope of this specification does not define an overall hardware or software system architecture to support hot plug. Instead, this specification only highlights the hardware elements that can be utilized to support hot plug for implementations. The system implementer shall consider the use of hot swap controllers on the +12V pins to prevent damage to the CMC card. Hot swap controllers limit the inrush current while also providing overcurrent, undervoltage and overvoltage protection capabilities.



5. Environmental and Regulations

5.1 Controller high altitude

Operational at 1500 meters above sea level

Non-Operational at 12192 meters above sea level

5.2 Controller relative humidity

Operating and Storage relative humidity: 10% to 90% (non-condensing)

5.3 Controller Temperature

Operating temperature range: -5°Cto +45°C

Storage temperature range: -40°C to +70°C

Transportation temperature range: -40°Cto +70°C (short-term storage)

Appendix

The ASPEED ast2400 and ast2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host (or from the network in unusual cases where the BMC console uart is attached to a serial concentrator). Therefore, some common vulnerabilities and exposures are caused by this mechanism, which can also be referred to CVE-2019-6260. This appendix addresses the CVE, and the relevant mitigation plan to the weakness. ***As long as the firmware code takes the suggestions as below mitigation, that any firmware code deck could prevent the BMC from the CVE attacks.***

CVE Item related to AST2400		**Suggested Mitigation Plan**	**Comments**
1	iLPC2AHB bridge Pt I	Can be disabled by configuring a bit in the BMC's LPC controller, see Pt II.	**Based on the suggested mitigation of CVE, ASPEED's advices**: Method to disable L2A bridge BUT still keeps Super I/O services: A. Set **HICR5** (1e789080h)[**08:08**] = **0**b B. Set **HICRB** (1e789100h)[**06:06**] = **1**b C. Set **SCU70** (1e6e2070h)[**20:20**] = **0**b Or H/W Strap [**20:20**] = **0**b Once L2A bridge is disabled, two designing-phase tools will **NOT** function; 1. ASPEED **SoCFlash** (ASPEED firmware update utility) 2. ASPEED **SLT** (System Level Test program).
2	iLPC2AHB bridge Pt II	Disable Super I/O decoding on the LPC bus (0x2E/0x4E decode). Decoding is controlled	**Based on the suggested mitigation of CVE, ASPEED's advices:**

		via hardware strapping and can be turned off at runtime, however disabling Super I/O decoding also removes the host's ability to configure SUARTs, System wakeups, GPIOs and the BMC/Host mailbox.	Method to disable L2A bridge **AND** disable Super I/O services: A. Set **HICR5** (1e789080h)[**08:08**] = **0**b B. Set **HICRB** (1e789100h)[**06:06**] = **1**b C. Set SCU70 (1e6e2070h)[**20:20**] = **1**b or **H/W Strap** [**20:20**] = **1**b Once L2A bridge is disabled, two designing-phase tools will **NOT** function; 1. ASPEED **SoCFlash** (ASPEED firmware update utility) 2. ASPEED **SLT** (System Level Test program).
3	PCI VGA P2A (PCI2AHB) bridge	Can be disabled by configuring one bit in the System Control Unit.	**Based on the suggested mitigation of CVE, ASPEED's advices:** Steps to disable PCI2AHB bridge: STEP 1. Update the **Host vBIOS** & **ASTSoC VGA 2D driver** to v1.03 or later version (The latest ASPEED vBIOS version is V1.08, Windows driver v1.06 and Linux driver v1.08) STEP 2. Set **SCU180** (1e6e2180h)[**01:01**] = **0**b Once PCI2AHB bridge is disabled, two designing-phase tools will **NOT** function; 1. ASPEED **SoCFlash** (ASPEED firmware update utility) 2. ASPEED **SLT** (System Level Test program)
4	UART-based SoC Debug interface	Can be disabled by configuring one bit in the System Control Unit. Separately, selection of UART5 via hardware strapping can prevent host-side access.	**Based on the suggested mitigation of CVE, ASPEED's advices:** Method to disable U2A: A. Set **SCU2C** (1e6e202Ch)[**10:10**] = **1**b (It's only applicable to AST2500 when AST2400 doesn't Have the U2A interface) Once U2A interface is disabled, one designing-phase tool will **NOT** function; 1. ASPEED **SoCFlash** (ASPEED firmware update utility)
5	DMA from/to arbitrary BMC Address-space via	X-DMA accesses are configured to remap into VGA address-	**Based on the suggested mitigation of CVE, ASPEED's advices:** Steps to block the X-DMA accesses from Platform_gX.s

	X-DMA	space in ASPEED uboot platform_gX.S files.	files or BMC firmware (recommended) STEP 1. Update the **Host vBIOS** & **ASTSoC VGA 2D driver** to **v1.03** or later version (The latest ASPEED vBIOS version is V1.08, Windows driver v1.06 and Linux driver v1.08.) STEP 2. Ensure the BMC firmware to integrate the latest Platform_gX.S file (v18) **STEP 3. Set SCU04 (1e6e2004h)[25:25] = 1b** STEP 4. Set **SCU180** (**1e6e2180h**)[**14:14**] = **0**b STEP 5. Set **SCU180** (**1e6e2180h**)[**06:06**] = **0**b Once X-DMA accesses is disabled, what ASPEED tool will be impacted; --- **None**
6	LPC2AHB bridge	Don't enable the feature if not required. Note: As a counter-point, this feature is used legitimately on OpenPOWER systems to expose the boot flash device content to the host	**Based on the suggested mitigation of CVE, ASPEED's advices:** Method to disable LPC_2_SPI A. Set **SCU2C** (**1e6e202Ch**)[**00:00**] = **1**b B. Set **HICR5** (**1e789080h**)[**10:10**] = **0**b **C. Set HICR5 (1e789080h)[08:08] = 0b** Once LPC2AHB bridge is disabled, what tool will be impacted; --- **None**
7	PCI BMC Device	Don't enable the feature if not required.	**Based on the suggested mitigation of CVE, ASPEED's advices**: Method to disable PCI BMC device **(IT IS DEFAULT DISABLED**) A. Set **SCU180** (**1e6e2180h**)[**08:08**] = **0**b Once PCI BMC Device is disabled, what ASPEED tool will be impacted: --- **None**
8	Watchdog setup	Ensure BMC reboots always use "SOC Reset" mode	**Based on the suggested mitigation of CVE, ASPEED's advices:** Trigger Watchdog with correct mode setup

			Reset system mode: Related bit-fields to reset system mode: → **WDT0C** (**1e78500ch**)[**06:05**] → **WDT2C** (**1e78502ch**)[**06:05**] →**WDT4C**(**1e78504ch**)[06:05] (**AST2500/AST2520 Only**) A. **00b SoC System**. (Default value during Power-on stage) → **AST2400/AST1250** would reset according to register **SCU9C.** → **AST2500/AST2520** would reset according to **WDT1C/WDT3C/WDT5C.** B. **01b Full Chip (Not recommended after development/validation phases)** → Would lead to the similar effect of **AC-cycle** or hardware SRST# signal triggering. What ASPEED tool will be impacted; --- **None**