NVL-AX RVP Hardware Architecture Specification

Revision 0.5
WW34’ 2025

Intel Confidential. For Internal Use Only.

Revision History

Rev#	Description	Date

Contents

List of Figures

List of Tables

Reference Documents/ Links

1. NVL-AX, HX, UPH & UL RVP PDT SharePoint link
2. NVL-AX/AM Engineering Docs link
3. NVL Platform Architecture Specification(PAS) link
4. NVL Platform MAS documents link
5. USB-C PD Add-In-Card, USBC PD Add-In-Card Specification Rev1_1_r2.docx, link TBD
6. Type-C USB Switching AIC - Cswitch Rev4.0, link TBD and Cswitch 2.0 link TBD
7. NVL-AX Platform CCB link (TBD)

Document Conventions

The terms NVL-AX/AM, processor and SoC are used interchangeably in the document.

Small letter ‘b’ stands for bits, e.g. Mbps stands for Megabits per second. Capital letter ‘B’ stands for Bytes, e.g. MB stands for Megabytes.

All binary numbers will have a suffix ‘b’ at the end of the number, e.g. 00110b. Hexadecimal numbers will be mentioned with a prefix ‘0x’, e.g. 0x11FD. Decimal numbers will not have any suffix or prefix.

Capital letter ‘HDR’ stands for Header in the figures.

Items mentioned as TBD are open and yet to be closed from the design perspective.

Acronyms

Acronym	Description
NVL	Novalake
PTL	Panther Lake
MTL	Meteor Lake
ARL	Arrow Lake
ADL	Alder Lake
AIC	Add-In Card
ALS	Active Level Shifter
BOM	Bill of Material
BP	Back Panel
BPK	Baltic Peak
BR	Barlow Ridge
BSSB	Boundary Scan Sideband
CC	Configuration channel
CIO80	Converged IO 80
CRLS	Cost Reduced Level Shifter
DCI-OOB	Direct Connect Interface Out of Band
DDR	Double Data Rate
DnX	Download and execute
DP	Display port
DPC	DIMMs Per Channel
dTBT	Discrete Thunderbolt
EC	Embedded controller
eUSB2	Embedded USB2
FP	Front Panel
GND	Ground return
HDMI	High-Definition Multimedia Interface
I3C	Improved Inter Integrated Circuit also known as Sense Wire
IIC or I2C	Inter-Integrated Circuit
iTBT	Integrated TBT
KoZ	Keep-out Zone
LSPCON	Level Shifter Protocol Converter

NOA	Node Observation Architecture
PCH	Platform Controller Hub
PD	Power Delivery
PD	Power Down
POR	Plan of record
PSS	Processor Secured Storage
RVP	Reference Validation Platform
RBR	Rood Bridge
SBU	Sideband use
SKU	Stock Keeping Unit
SML/SMB	System management link/Bus
SODIMM	Single Outline Dual Inline Memory Module
SPI	Serial Peripheral Interface
TBD	To Be Decided
TBT	Thunderbolt
TCPC	Type-C port controller
TCPs	Type-C ports
TCSS	Type-C sub system
THC	Touch Host Controller
UFP / DFP	Upstream/Downstream Facing Port
USB	Universal Serial Bus
VBUS	Bus power
VISA	Visualization of Internal Signals Architecture
WIP	Work In Progress
XDP	eXtended Debug Port

1. Introduction

The scope of this document is to cover the overall functional architecture for the NVL-AX/AM RVPs including the debug and validation hooks. The document would describe the architecture and feature set of NVL-AX/AM RVP's and the design in detail.

1.1. Design Team

The Key contacts for NVL-AX/AM RVP are given below.

Table 1: Key Contacts for NVL-AX/AM RVP design

Role	Point of Contact
RVP Program Manager, Systems PDT, Boards & Kits	Nalbalwar, Sachin Madhavrao
RVP Engineering Manager	M, Manjunatha B
RVP Architect	Sharma, Deepak Srighakollapu, N V S Kumar (PD Architect)
RVP Design Lead	Kss, Ranganadh
RVP Design Engineers	Bhagat, Rekha K S, Vachana M, Chethan E S, Gokul
RVP Power Delivery Lead	M, Manikandan1
RVP PCB Layout Lead	B, Velmurugan Chandran, Monisha
Mechanical Team	A, Bhavaneeswaran Kaja, Ajmeer
Validation Lead & CSF	TBD

1.2. RVP Strategy

RVP strategy is available at NVL PDT SharePoint site. The link is 01_NVL_AX_RVP_Strategy

1.3. RVP design SKUs

The NVL-AX/AM RVP will have the SKUs as listed below. There will not be a different PI / PnP Board SKUs rather all the boards will have same implementation from PI / PnP perspective. All RVP boards will have PnP HDR as place holders; however, only PnP BOM SKU RVPs will be stuffed with 2x7 PnP HDRs.

Table 2: NVL-AX/AM RVP SKU details

Base Board#	RVP SKU	Base board SKU/ BOM SKU	PI/ LL Target	Validation Config	SoC Support	PCH IOE Support	Memory Support	PCB Type (POR L# + RVP L#)
RVP 01	NVL Ax/Am LP5x MOP T3 with PCH IOE RVP	Base Board SKU		Volume runner	AX/AM	With Out PCH IOE	LP5x MOP	Type-3, 10L+6L
		BOM SKU		PnP SKU		With Out PCH IOE		
		PPV Board SKU		PPV		TBD		
		BOM SKU		SIV		With PCH IOE		
		BOM SKU		ECG		With PCH IOE		
		BOM SKU		Memory DV		TBD		
		BOM SKU (Placeholder) for AM				TBD		

2. Feature Set & HW-BOM

2.1. RVP Landing Zone

RVP landing zone is available at NVL PDT SharePoint site. The link is 02_NVL_AX_RVP_LZ_PRD

2.2. Platform HW BOM

The platform HW BOM is being defined at the HSD-ES links below.

https://hsdes.intel.com/appstore/carbon/bom/parts-manager/22019692237

2.3. Platform Validation Configuration

The platform validation configurations can be found in the below link.

NVL-AX Validation configuration NVL-Ax Validation Configuration Ver 0.5.xlsx

3. General Architecture

3.1. Platform Block Diagram

The functional block diagram of the NVL-AX/AM RVP system with all the interface routing and connectivity options are presented in below figure. All the major interface options are mentioned in it. The validation hooks are not illustrated in the figure but will be covered in the design. The details of the validation hooks provided are covered in the respective sections.

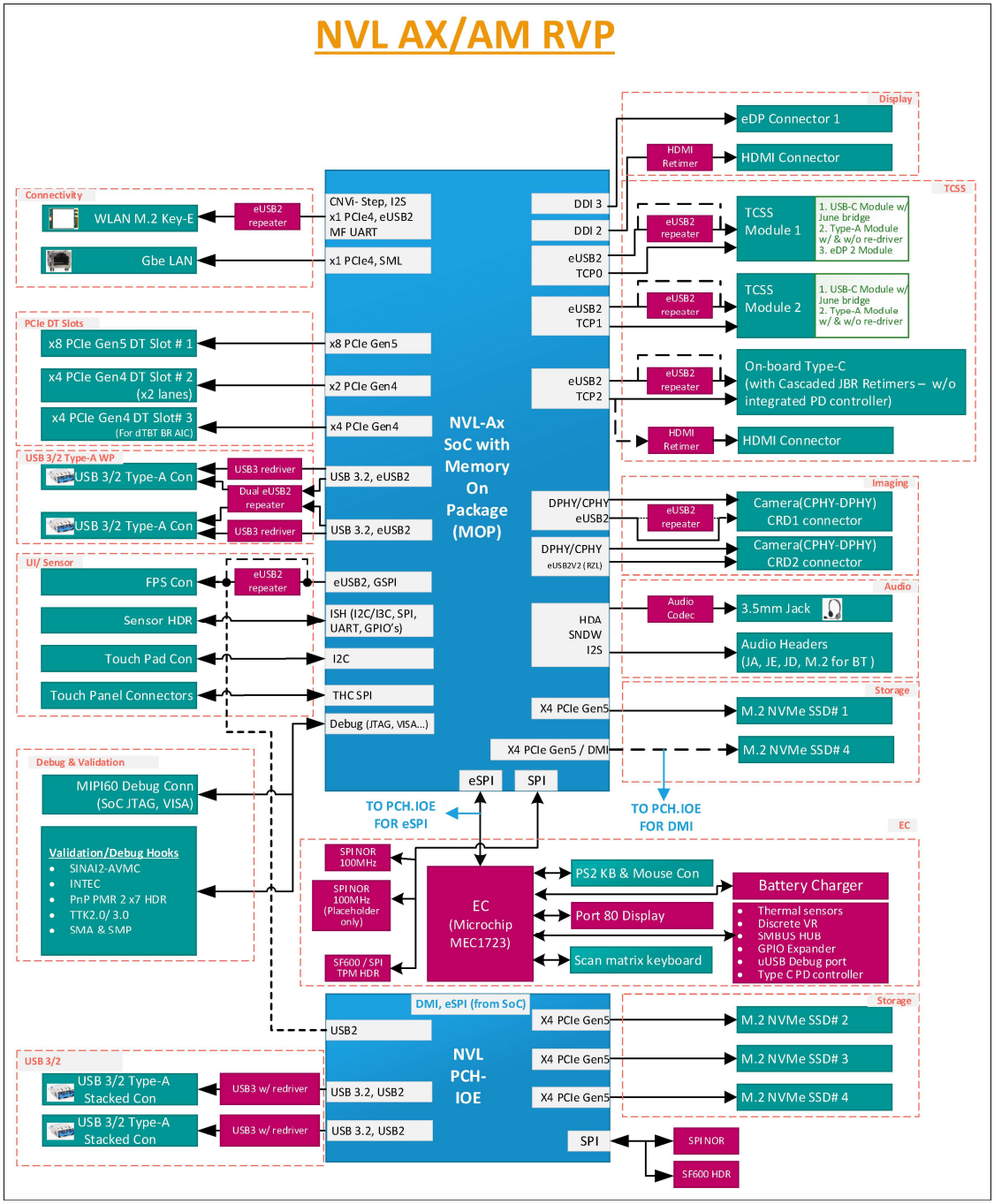


Figure 3-1: NVL-AX/AM RVP with PCH IOE

3.2. Novalake AX/AM SoC overview

NVL-AX/AM SoC is supporting die disaggregated strategy (Compute/Gfx/HUB/PCD-H). C-Die and GFx die connects to the Hub die using an FDI connection. Similarly, Hub Die connects PCD-H die also using FDI connection. PCD-H stands for Peripheral Controller Die-H and it contains all the traditional client IPs.

NVL-AX/AM have new core architecture (PCore: PantherCove (PNC), ECore: arcticwolf (ARW), CPU Die contains the central compute cores, the LLC caches, the ring that connects all the cores and provides coherency and the connection to the memory subsystem (via the Hub).

Graphic support is from a stand-alone graphics die connected to the HUB die with a dedicated foveros connection.

For more details, please refer NVL SoC overview HAS , NVL-AX SoC overview HAS and NVL Product Specification HAS

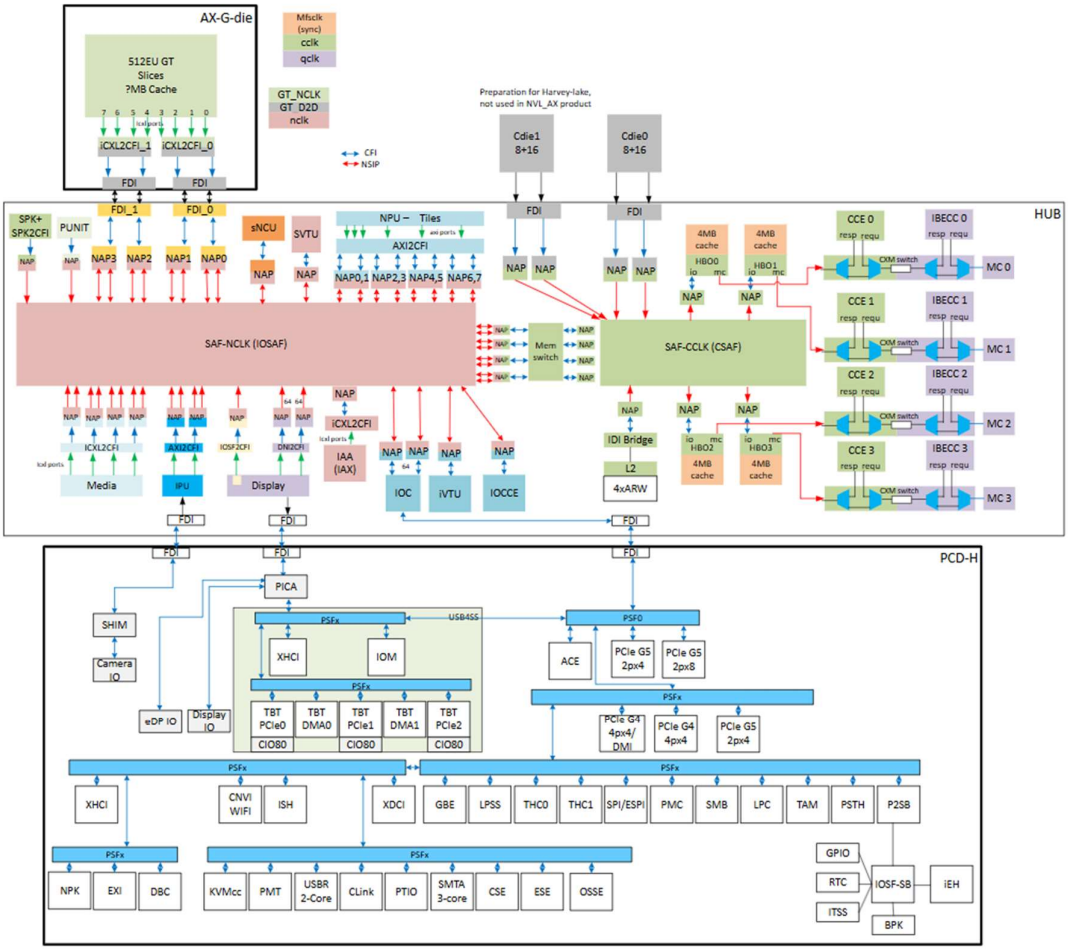


Figure 3-2: NVL-AX SoC Block Diagram

3.3. NVL-AX/AM platform SoC/Interface support overview

Below table Show AX/AM RVP Supported CPU TDP Characteristics.

Table 3: NVL-AX/AM RVP Supported CPU TDP Characteristics

Die Package	Product	TDP
NVL-AX	8+16+4+GT (512EU), NPU7 (6 Tiles)	Nominal TDP (PL1): 65W, PL2: 125W? TBD
NVL-AM	4+8+4+GT (256EU), NPU7 (6 Tiles)	Nominal TDP (PL1): 40W, PL2: 64W? TBD

The major platform interface supported on the NVL-AX/AM RVP apart from debug, sideband and GPIO are listed below.

Table 4: NVL-AX/AM SoC, RVP platform interface support summary

Interface Source	Interface	NVL-AX/AM SoC and PCH
NVL-AX/AM SoC	**Memory**	LP5x MOP
	eDP/ DDI	1x4 eDP1.5 and 1x4 HDMI 2.1
	Concurrent Dual eDP Display	N/A (Optional with eDP/Type-C)
	USB Type C	3 ports CIO80: supports USB4.0 + TBT5 + DP 2.1 + HDMI2.1
	MIPI CSI	3 concurrent D-PHY/C-PHY 2.1 to 2.5Gbps
	SoC-PCIe	24 Lanes (16 G5 lanes and 8 G4 lanes), 9 Root Ports, 9 Clocks
		PEG Gen5: 1x8 [1x8, 2x4]
		2x4 Gen 5 for Storage
		2X4 Gen4 for Barlow, SD card, WLAN, LAN
	GbE (Muxed PCIe)	1x 1GbE Port (muxed with PCIe Gen4 port)
	USB3.2 Gen2x1 10G	2 ports
	eUSB2	8 ports eUSB 2.0
	CNV (WiFi / BT)	Integrated 2x2 Wi-Fi 7 (802.11ax R2 w/ CDB) and Bluetooth 6
	SPI Interface	1 CSME SPI
		2 THC SPI
	Audio	1 HD-A
		3 I2S
		4 Sound Wire
		2 DMIC Interfaces
	eSPI	eSPI with 4 chip select signals
	LPSS	6 I2C Ports
		2 I3C
		2 GSPI/THC Ports
		3 UART Ports
	ISH	3 I2C Ports
		1 SPI Bus
		2 UART Ports
	Thermal DIODE	PCH Thermal Diode
	MLINK	1 Channel with CLK, DATA & RST
	Integrated Clock Controller (ICC)	9 ref CLK & CLK req (All Gen5)
	SMBUS / SMLINK	2 SMLINK and 1 USBC_SMLINK
NVL-S PCH IOE	**PCH-IOE PCIE**	24 lanes, 12 Gen5 lanes and 12 Gen4 lanes
	PCH-IOE USB3.2	10 USB3 Gen2,
	PCH-IOE USB2	14 USB2
	PCH IOE-eSPI	1 eSPI
	PCH-IOE SPI	1 SPI
	PCH-IOE Clock and CLK REQ	12 ref Clocks (8 G5 and 4 G4)
	PCH-IOE GPIO	In AX/AM RVP GPIO usage limited to support's HSIO features from PCH IOE
	PCH-IOE GPIO LPSS	In AX/AM RVP No support for LPSS interface.

3.4. Form Factor

NVL AX/AM RVP formfactor is listed in the table below. Please refer to the Mechanical chapter for more details.

Generic Implementation Notes

- GND vias are spread across the board on both top and bottom sides, with clear marking on silk screen will be provided.
- All the socket caps will be specified in the schematics and can be removed in the customer version of the schematics or board.
- RVP design will follow the PDG for routing of all traces.
- All the LED will be placed on the TOP side and will be visible.

Table 5: RVP Formfactor

Si#	RVPs	PCB (Type/ Layer count/ material) & PCB size
1	**RVP 01**	T3, 10L+6L, Premium mid loss 12”x10”

4. Main Memory

4.1. Overview

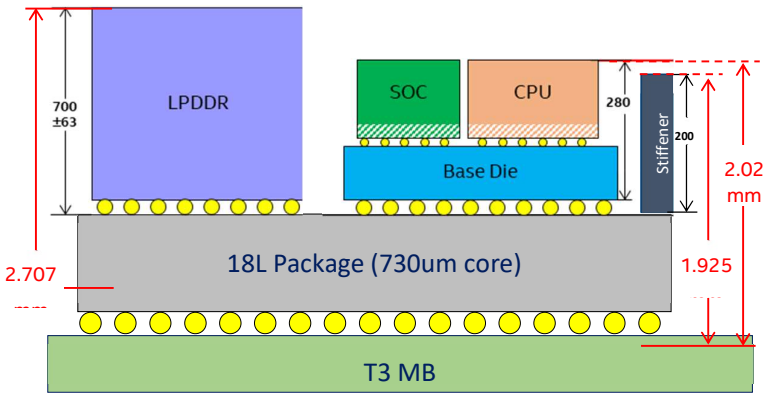
The NVL AX/AM supports LP5x Memory on package (MOP). It Supports 256 bits (64 x4 channel).

Attribute	NVL-AX & AM
PKG Size (X,Y)	56.5x37.5
Ball Count	4326
Ball Pitch	0.65mm
BGA Solder Type	SAC 305 16mil, Cu core ball 10mil
Layer Count	18L
Core Thickness	730
Substrate Thickness	1.419 (18L)
Base Die Size (Physical size)	45448.52x14039.96um(AX) 33454.58x14039.96(AM)
Base Die Bump Pitch	110um (Min)
SOC Die Thickness	280um
Stiffener	Yes (200um)
DSC/LSC	LSC 0204 XLP x 16 Thermistor(N74463-001) (XYZ: 0.4x0.2x0.2+/-0.02mm)
Z height (top of SOC die)	2020 um
Z height (top of Stiffener)	1925 um
Z height (top of Memory Die)	2712 um (Max) 12.4x7mm, 563balls
Minimum MB technology	Type-3
Total IO	635
Total CTF IO	449

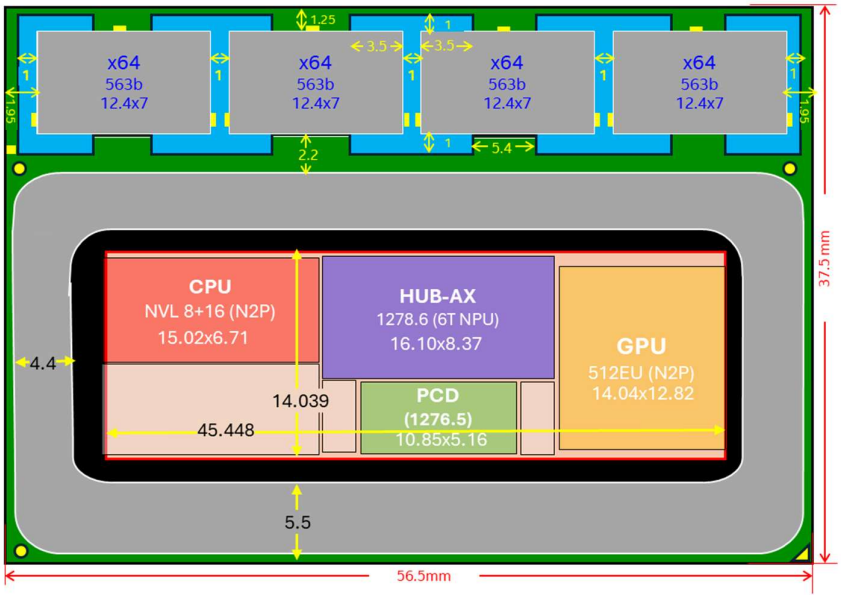
Z-Height at top of CPU	Nom	±
Top Chiplet	160	18
Chiplet FLI gap	36	
Base Die	84	
Chip Gap	35	5
Substrate (730um SC)	1419	TBD
16 mil BGA (pre-SMT)	286	50
Total	2020	73

Z-Height at top of Mem	Nom	±
DRAM (max)	915	63
DRAM Chip Gap	92	15
Substrate (730um SC)	1419	TBD
16 mil BGA (pre-SMT)	286	50
Total	2712	128

Z-Height at stiffener	Nom	±
Stiffener	200	20
Sealant gap	20	20
Substrate (730um SC)	1419	TBD
16 mil BGA pre-SMT	286	50
Total	1925	128



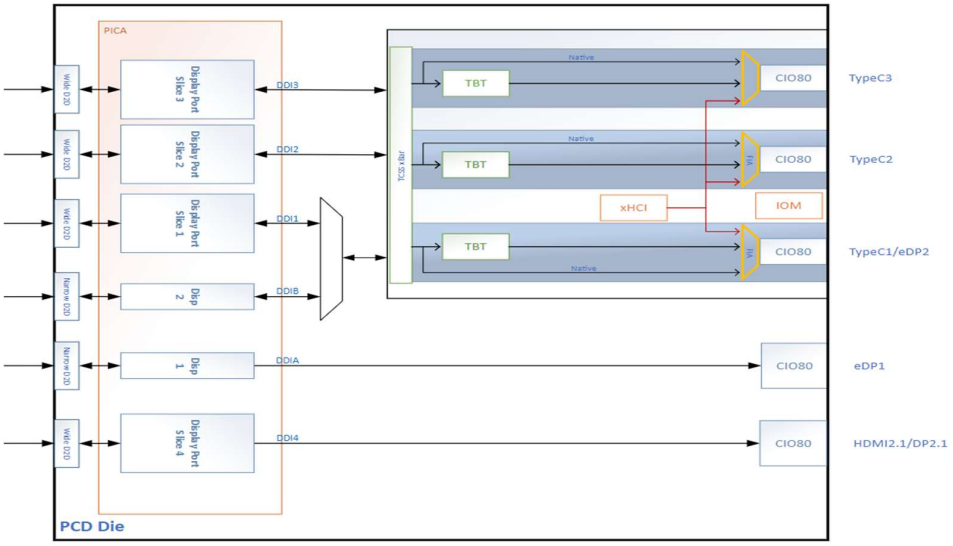
NVL-AX


1.25
3.5
3.5
1
x64
563b
12.4x7
x64
563b
12.4x7
x64
563b
12.4x7
x64
563b
12.4x7
1.95
2.2
5.4
CPU
NVL 8+16 (N2P)
15.02x6.71
HUB-AX
1278.6 (6T NPU)
16.10x8.37
GPU
512EU (N2P)
14.04x12.82
PCD
(1276.5)
10.85x5.16
4.4
14.039
45.448
5.5
37.5 mm
56.5mm

5. Display

5.1. Overview

NVL consists of CIO80 PHY or Lake Tahoe PHY(LTPHY) for display interface. The same PHY is used in TCSS and Dedicated display. NVL PCD-H die supports three specifications: DP2.1 (RBR, HBR1-3, UHBR10/20), HDMI2.1 and EDP1.5. The main block inside of the Display Engine is the Display Pipe which contains multiple planes. Each plane reads data from memory, formats it into pixels, and can apply color correction and scaling. IP can support up to four simultaneous displays (pipes A, B, C, D).



PCD-H

The diagram shows the mobile display subsystem in PCD-H.

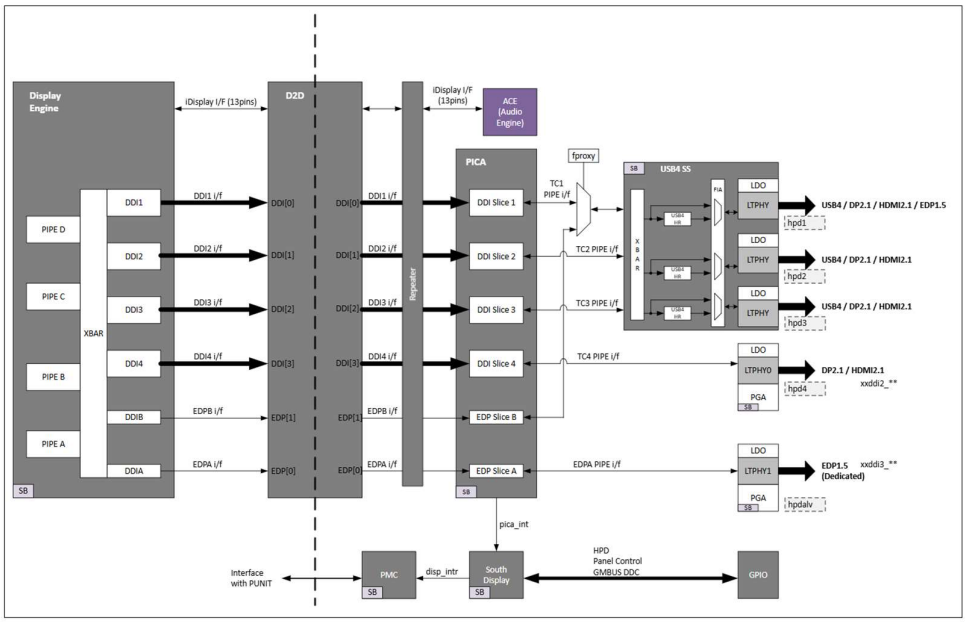


Figure: NVL Mobile PCD-H Display Subsystem (source)

5.2. Display domain platform MRD/PRD

Below are the platform MRD/ PRD for the display domain.

- Platform MRD HSD link.
- Display Domain platform PRD HSD link.

5.3. Display domain RVP LZ/ PRD

TBD

5.3.1. NVL RVP Display Topology port mapping

Refer to the table below and block diagrams for NVL RVP's eDP/DDI display port configuration.

Table 6: NVL-AX/AM RVP's eDP/DDI port display configuration

Silicon Interface	NVL-AX/AM RVP
DDI-3	eDP Panel Conn1
DDI-2	HDMI 2.1 native Con (HDMI 2.1 @12Gbps w/ retimer)
TCP0	eDP Panel Conn2 (Via TCSS Module)/ HDMI 2.1 Re-timer/Redriver (via TCSS module)- For NEX Team
TCP1	HDMI 2.1 Re-timer/Redriver (via TCSS module))- For NEX Team
TCP2	On board Type-C Cascaded June Bridge Re-timer/ HDMI 2.1 Native con (Option with Tripad)

5.4. HW BOM

Below are the hardware BOM items used in Display validation on NVL RVP.

Table 7: Platform HW BOM

Sl No	BOM Requirement	Part/IPN	Part number	Vendor
1	**eDP 1.5 Panel**	BOM51A, BOM54,BOM57,BOM58, BOM60	ATNA40HQ02-0 NS153B9M-K61 LQ0DASF527	SDC BOE Sharp
2	**HDMI 2.1 @12G Display**	TBD	TBD	TBD
3	**HDMI 2.1 redriver**	N40003-001	PS8219QFN46ITR-B0	Parade
4	**HDMI 2.1 retimer**	K90061-003	PS8419QFN46GTR-A1	Parade

5.5. AIC List

Below table shows the AIC supported on NVL RVP's.

Table 8: AIC supported on NVL RVPs

Si#	Add In Card (AIC) Description	IPN	Rev #	Wiki link
1	eDP mux AIC for enabling display MUX between internal graphics (iGFx) and external graphics (Dgfx)-TBD	TBD	TBD	TBD
2	eDP TCSS module	TBD	TBD	TBD
3	DP 2.1 with retimer TCSS module	TBD	TBD	TBD

5.6. Display Topology

Display and display muxing topology for NVL is captured in below section.

5.6.1. NVL RVP Display Topology block diagram

Below image shows high level block diagram for display implementation on NVL.

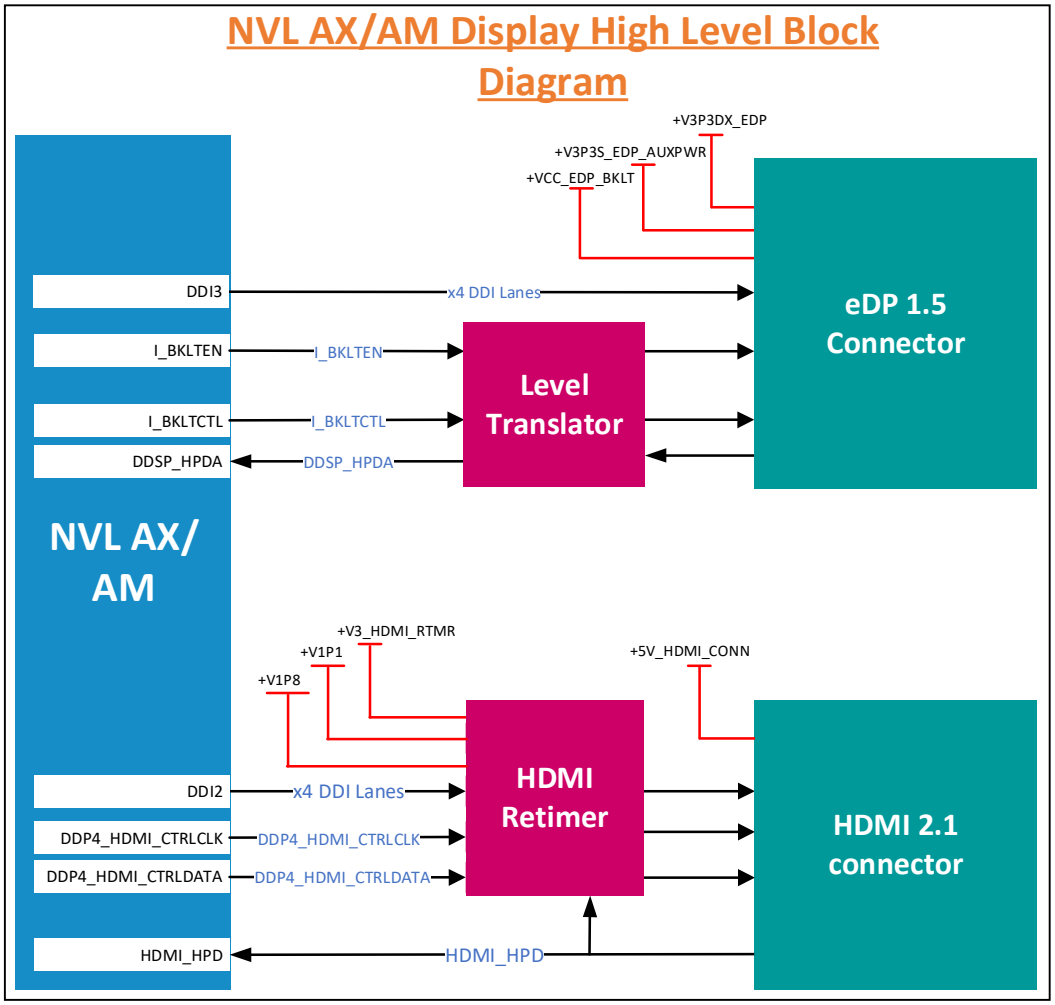


Figure 5-1: DDI Display implementation

5.6.2. NVL RVP eDP Display mux Topology (TBD)

RVP supports display shift feature through eDP MUX AIC.

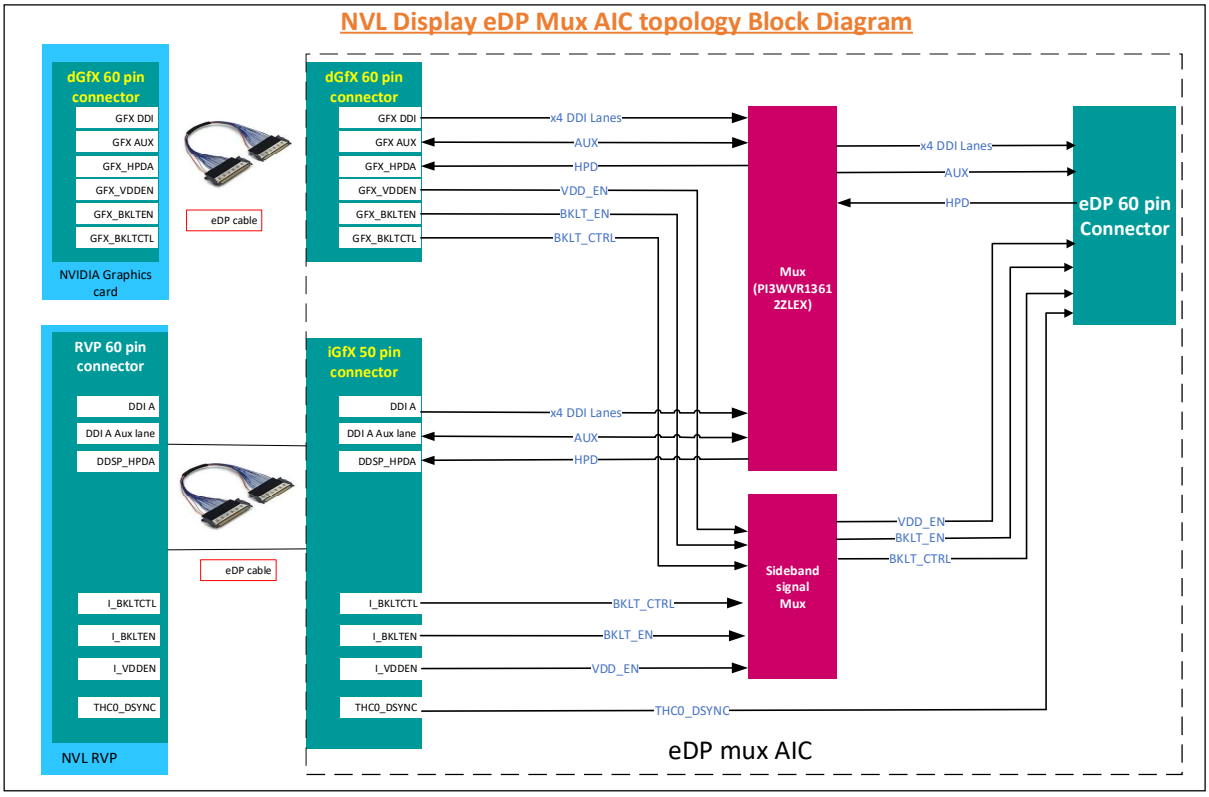


Figure 5-2: NVL RVP eDP Mux Topology

5.6.3. NVL RVP DP 2.1 Retimer Mux topology to BR AIC (Via TCSS Module)

DP2.1 Retimer Mux topology in NVL RVP to provide display signals to BR AIC. Support will be through a DP 2.1 Retimer AIC on TCSS module.

5.7. Display Topology from TCSS ports

Please refer to the Type-C and thunderbolt section for display topology support from TCSS.

5.8. DG Support

RVP will be supporting 3rd party graphics card from Nvidia or AMD, and the Intel DG MRB AIC is not PoR.

5.8.1. 3rd party Graphics card support on x8 PCIe slot

RVP supports the CLKREQ muxing between pins B12 and B17 of the PCIe slots to enable the L1 sub-state for low power modes of the 3rd party PCIe AICs. The default routing of CLKREQ on PCIe 8 lane slot will be to pin B12 of the PCIe slot with a switch option provided on the board to change the connection to pin B17 of the slot.

Additional pins supported for external GFx cards are listed below.

Table 9: Sideband signals for external GFx card support

Pin	Signal Name	Description	I/O (PCIe slot)	Polarity (Default)
A19	**DGPU_PWR_EN#**	Used to control power enable for GPU. Set to 0 by default. Option provided for having both logic low and logic high for this A19 pin through switch.	I	Low
B30	**DGPU_SEL**	Used in conjunction with GPU_PWR_EN# to control power state transitions in GPU; 0 = DGPU select. 1 = DGPU deselect. B30 is an input at the PCIe slot and is Active Low.	I	LOW
B12	**DGPU_CLK_REQ#**	Allows dynamic control on CLKREQ to hit power saving features on new designs.	O	LOW
A11	**DGPU_RST#**	Discrete GFx Enable signal. Controlled by Switchable Graphics Driver and driven by PCH GPIO. Used to gate with Platform Reset to enable the Reset for dGPU. 0 = Keep dGPU in reset; 1 = Reset is released. This action taken 100ms after DGPU_PWROK to ensure clock is stable.	I	LOW

5.8.2. PCIe CEM implementation on RVP (DG)

Below image depicts DGFx implementation on RVP.

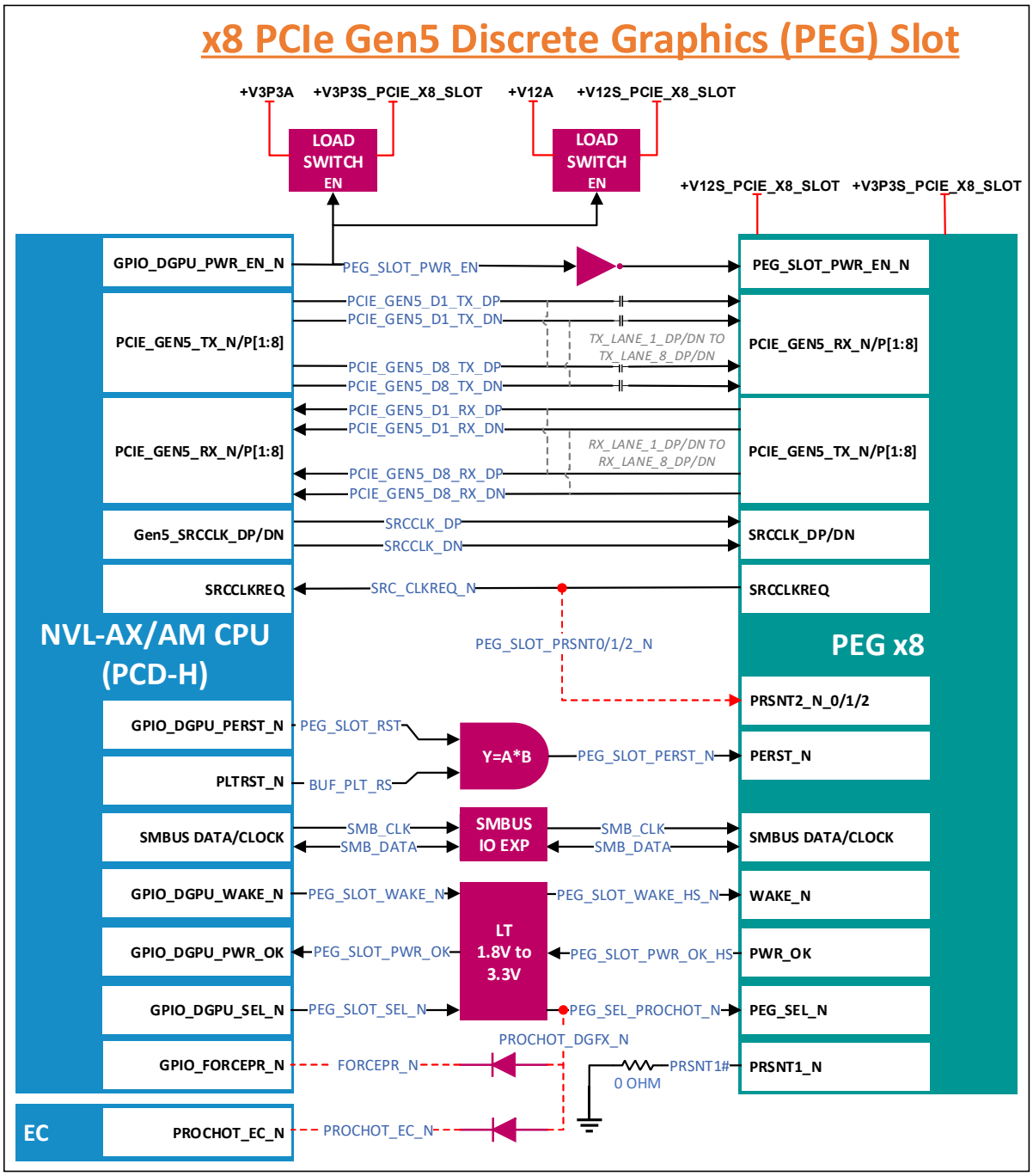


Figure 5-3: PCIe CEM implementation on RVP

6. Type-C & Thunderbolt

6.1. Overview

NVL AX/AM supports integrated three Type-C ports, supporting DP2.1, USB3.2, TBT3, TBT4, TBT5 and USB4 protocols. eDP over Type C is supported on NVL AX/AM RVP on TCP Port0. NVL-AX/AM has Integrated 80G (CIO-80) enabling support for USB4v2. Compared to USB4 v1.0, USB4 v2.0 uses the same number of lanes with double the bandwidth per lane. For NVL AX, USB4SS is integrated in PCD die. USB4 Port Configuration: 3 Type-C Ports.

Note: Gen-T is no longer POR for NVL PCD-H, PCD-S.

6.2. Type-C & Thunderbolt domain platform MRD/PRD

Below is the platform MRD/ PRD for the Type C domain.

- Platform HSD link.
- Type C Domain platform PRD HSD link.

6.3. Type-C & Thunderbolt Features Supported (RVP LZ/ PRD)

6.3.1. RVP PRD for Type C and Thunderbolt

TBD

6.3.2. NVL AX/AM Type C and Thunderbolt Domain LZ support

Table 10: Type C Main Features supported in NVL AX/AM

Si#	Domain features	NVL-AX/AM RVP
1	**Number of USB-C/ TBT ports**	3x port
2	**TBT5 80G/40G w/ single retimer (June bridge) via TCSS Single Module**	Supported, June Bridge TCSS Module
3	**TBT5 80G/40 w/ single retimer (June bridge) via TCSS Dual Module**	No support
6	**TBT5 80G w/ single retimer (June bridge) MB down**	No support
7	**TBT5 40G w/ single retimer (June bridge) MB down**	No support
8	**TBT5 80G w/ cascaded dual retimer (JBR+JBR) MB down**	Supported
9	**TBT5 80G w/ cable topology MB solder down/ TCSS Module**	No support
10	**TBT5 80G w/ single retimer (Rood bridge) via TCSS Module**	No support (ZBB'd)
11	**TBT 80G/40G Mix topology**	No Support

12	**Barlow Ridge dTBT Support w/ dGFx MB solder down**	No support
13	**Barlow Ridge dTBT Support w/ dGFx via BR AIC**	1x Barlow Ridge (BOBCAT) AIC
14	**iGfx DP2.1 to BR AIC via TCSS DP Module**	Supported

Table 11: Type C Auxiliary Features supported in NVL AX/AM

Si#	USB-C domain other features	AX/AM RVP
1	**I3C Debug (SoC) mux capability on Type-C port**	ZBBed in NVL
	I3C Debug (EC)mux capability on Type-C port	No support
2	**USB2/3 Dbc debug support**	Supported
3	**DnX Support**	No Support
4	**VPRO support**	Supported
5	**Type-A WP Con USB 3.2 Gen2 x1 10G redriver less**	2x port, via TCSS Module (TBD)- RVP length to be analysed
6	**Type-A WP Con USB 3.2 Gen2 x1 10G w/ redriver**	2x port, via TCSS Module.
7	**June Bridge flash sharing support**	TBD
8	**eUSB2 repeater single port (Common Footprint)**	3x Port support
9	**eUSB2 repeater dual port (Common Footprint)**	Supported on CPU USB3.2 Type A MB Ports
10	**eUSB2 repeater with PD support (Dual PD + Dual repeater - CFP)**	Supported over Modular TCSS
11	**ThunderCat4**	Supported
12	**ThunderCat5**	Supported
13	**USB PD support**	2x 48V EPR with TCSS module. 48V EPR MB Down (Cascaded June Bridge Port)

6.3.3. NVL AX/AM Type-C and Thunderbolt Port Mapping

Refer to below table and block diagrams for the NVL AX/AM RVP TCSS Type-C configuration.

Table 12: NVL AX/AM RVP's TCSS Type-C Port Configuration

Silicon Port	NVL AX/AM RVP
TCP0 (TBT 80G/ eDP2)	**M.2 Modular TCSS** (single module) **USB PD: 48V EPR:** 1. w/June w/PD (default)
TCP1 (TBT 80G)	**M.2 Modular TCSS** (single module) **USB PD: 48V EPR:** 1. w/June w/PD (default)
TCP2 (TBT 80G)	Type C Con - TBT 80G **w/ cascaded** dual June bridge **solder down** **USB PD: 48V EPR. PD Controller TBD**

6.4. HW BOM

Below Table indicates the Hardware BOM list for Type C Interface.

Table 13: Type-C HW BOM

Si#	HW BOM Description	Part#/ IPN	Vendor
1	**Type-C TBT5 80G retimer w/o PD**	June Bridge MPN: (TBD)	Intel
2	**Type-C TBT5 80G discrete TBT controller chip**	Barlow Ridge MPN: 99CJDR IPN: M94480-028	Intel
3	**Single port PD controller CFP2.0**	TI: TBD Realtek: RTS5452P-20E-GR	TI/Realtek
4	**Dual port PD controller CFP2.0**	TI: PTPS669982BAZBJT Realtek: RTS5453P- 20E-GR	TI/Realtek

6.5. Type-C AIC/ TCSS Module LIST

Below is the list of AICs supported in Type C domain on NVL-AX/AM RVP.

Table 14: TCSS Modules/ AICs support on NVL AX/AM RVP SKUs

TCSS Modules	TCSS Card Details	Status	PD controller	Type C Port Supported	Card Number
eDP over TCP	eDP TCSS Module	Reuse from PTL	NA	TCP0	500
	June Bridge 80G TCSS single module + **3rd Party PD** controller	New Design	Realtek/TI	TCP0, TCP1	107
Type-A Modules	USB3/2 Type-A TCSS Module Re-driverless	Reuse from PTL	NA	TCP0*, TCP1*	600
	USB3/2 Type-A eUSB2 repeater TCSS Module (Soft Collaterals)	New Design (only for customer reference eUSB2 ICs)	NA	TCP0*, TCP1*	NA
	USB3 Type-A Redriver topology	New Design	NA	TCP0, TCP1	601
DP Module	TCSS DP 2.1 Module	New Design	Parade retimer	TCP0, TCP1	401
HDMI Module	TBD	TBD	TBD	TCP0, TCP1	TBD

Note:

1. **All modular TCSS AICs are 'plug and play' in G3 state only.**
2. High power eDP panels (above 11.1 W) are not supported on the eDP module.
3. * - Type A module (redriverless) support based on layout length constraint.

For more details on modular TCSS AICs and user guide, please refer below link:

https://goto/tcssmodule. (User guide is available in same link.)

6.6. Type C & TBT high level Block Diagram

Below image shows high level Block Diagrams of Type C and TBT implementation on NVL AX/AM RVP.

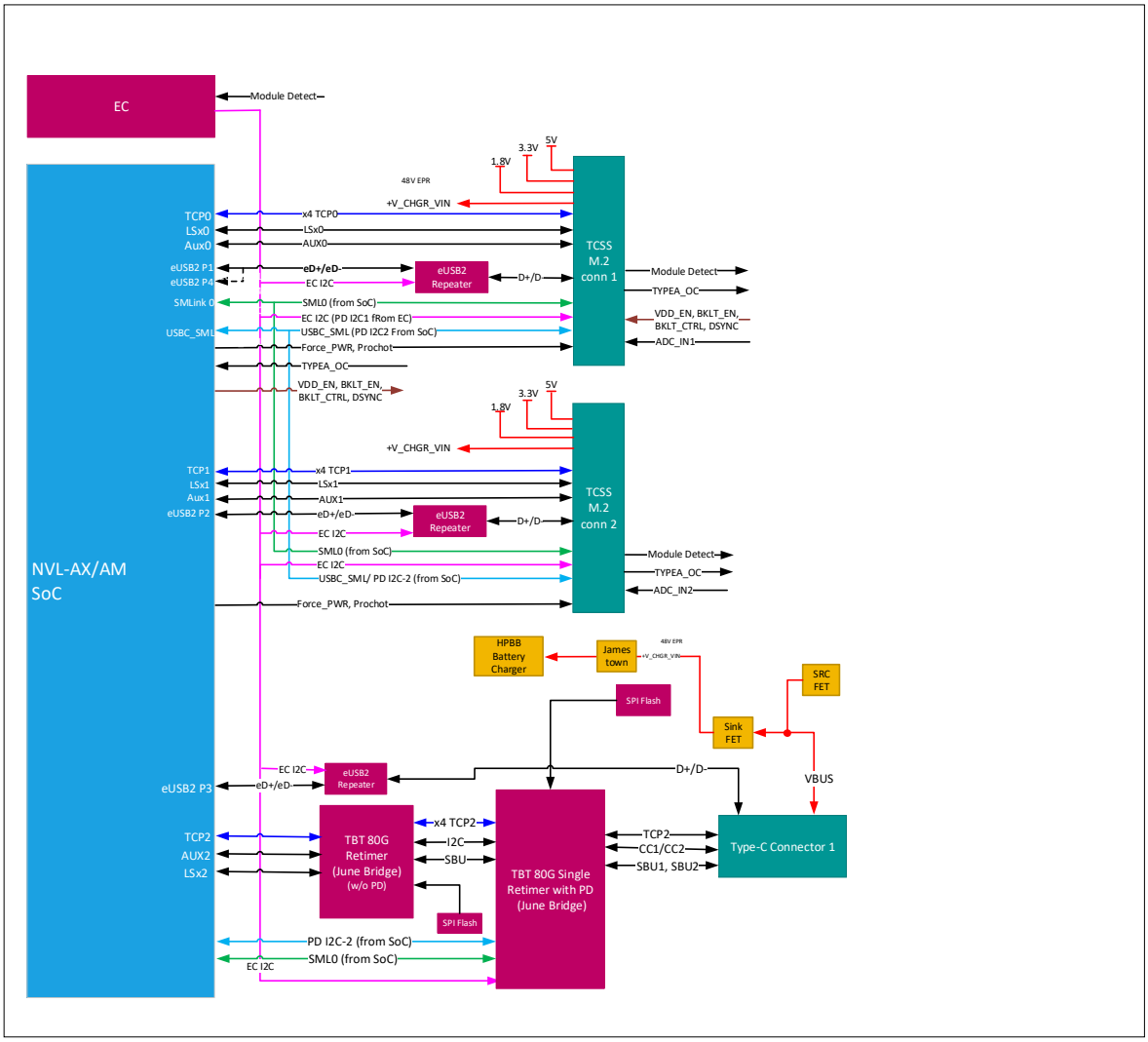


Figure 6-1: NVL AX/AM RVP - Type-C High Level Block Diagram.

6.7. I3C debug

I3C Debug (SoC) is ZBBed for NVL. Please refer to the link for more information.

6.8. TBT Retimer and Flash support

- The SoC output is a muxed port that supports TBT5/TBT4/DP2.1/HDMI2.1/USB3.2/USB4 protocols. PCIe is not supported as native or alternate mode.
- To support TBT protocol at 80Gbps, TBT retimer is implemented on the path. Each integrated TBT type-C port requires a retimer in NVL AX/AM RVP. Aux, LSx signals are routed to the retimer where they are muxed internally.
- SML0 from SoC is connected to Retimer for vPRO support over TBT dock.

6.8.1. Thunderbolt Retimer

June Bridge (JBR) is TBT5 (80G) Retimer without Integrated PD controller support.

RDC link for June Bridge (JBR) Datasheet – **843990**

6.8.2. Retimer Flash Sharing

NVL AX/AM RVP supports Cascaded June Bridge Retimer topology where flash is not shared between the retimer. Each retimer will support the separate flash.

SF100-dediprog header shall be provided for shared Flash initial programming. Below are the details of Dediprog Header.

- 1.27mm pitch 2x3 header is provided on RVP.
- Need Universal Adapter board and cable for programming - https://www.dediprog.com/product/ISP-ADP-127
- Cable as 2x4 header and Last two pins are NC in it. Hence leave last two pins unconnected and connect just 6 pins as below.
- Flash to be programmed in **RVP powered OFF**, Dediprog will be Master and 1.8V from the Dediprog shall be used on RVP

SF100 1.27mm 2x4 Header Pin Out

1	Vcc	GND	2
3	CS	CLK	4
5	MISO	MOSI	6
7	Vpp/Acc	I/O3	8

No Connect

This FW programming needed only when the TBT interface is not up (initial stages of bring-up). Once the TBT interface is up and working, programming through a host is possible.

Alternatively, unstuffed independent Flash footprint will be provided for the Slave retimer when flash is shared on the board.

6.9. PD Controller Support

1. TI/ Realtek CFP2.0 PD Controllers will be supported over TCSS modules.
2. Barlow Ridge AIC will use PD AIC with TI PD Controller. In NVL AX/AM we will use - BR AIC V2.1+PTL CFP 1.0 w/ SCVR PD AIC.
3. Mother Board Down Port PD Controller TBD

6.9.1. PD Controller Communication

PD controller communication could be over I2C or through GPIOs as below:

- PD (slave) to EC through I2C communication for UCSI communication (I2C1)
- PD (slave) to PMC through USBC SML Communication (I2C2)
- PD (master) to TBT retimer for configuration (I2C3)

The I2C addresses for various PD controllers (TBD)

6.9.2. PD and Retimer Debug Support

All the RVP SKUs supports following header for debug purposes. By default, all the debug headers paths are enabled.

1. Individual JTAG headers (HDR_2X3) on all the retimers – present on RVP
2. 2x4 Header (IPN: N26669-001)

Table 15: 2x4 header1 Debug / programming pin mapping

Pin #	Signal Name	Pin #	Signal Name
1	PMC PD I2C SCL	2	EC PD I2C SCL
3	PMC PD I2C SDA	4	EC PD I2C SDA
5	PMC PD I2C INT	6	EC PD I2C INT_N
7	PROCHOT_N	8	GND

6.9.3. PD GPIO Configuration

TBD

6.10. Discrete TBT Barlow Ridge support

Barlow Ridge Device/Hub is a USB4 Ver2 controller that acts as a Hub or a point of exit in the USB4 Ver2 domain. USB3, PCIe and DisplayPort protocols are encapsulated into the USB4 fabric and can be tunneled across the USB4 domain. The Barlow Ridge Thunderbolt controller also acts as a flexible re-timer for DP protocol, or a USB3.2 Hub. For more details on Barlow ridge please go to link.

Barlow Ridge USB4 connection data rate is 40Gbps per lane (supporting overall TBT 80G / 120G speeds) and is compatible with USB4 Ver2 specification enabling USB4 link at Gen4, as well as backward compatible with Gen3 and Gen2 lane speeds.

6.10.1. Power and data path on Barlow Ridge

Below figure shows the power and data path block diagram on Barlow Ridge controller.

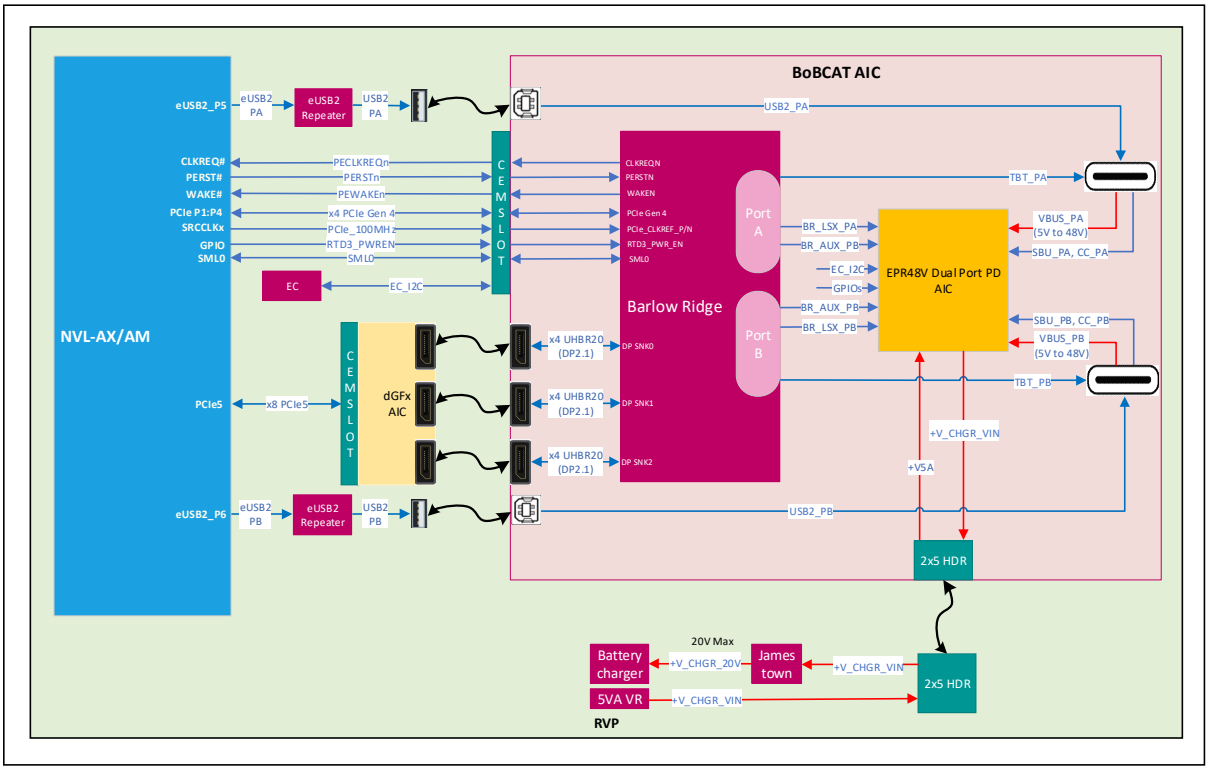


Figure 6-2 : Barlow Ridge AIC High level block diagram

Note:

1. BR AIC V2.1 + PTL CFP 1.0 w/ SCVR PD AIC.
2. BR AIC will be a rebuild with LSX level shifter bypass.

Below table lists down support for Barlow.

Table 16: NVL AX/AM TCSS Type-C Port Configuration

Interface/ Feature	AX/AM RVP
PCIe Gen5 #	1. dGFx support via x8 PCIe Gen5 CEM Slot 2. 1x No's - Barlow Ridge dTBT Support w/ dGFx via BOBCAT AIC
Barlow Type C PD Support	48V/20V No 28V and 36V support

6.10.2. iGPU support over barlow ridge

To properly support UHBR20 rates from dGPU and iGPU, an active (retimer-based) MUX is required. For mobile workstation and gaming systems, customers are looking for dGPU and iGPU connectivity through TBT5 ports. The PS8481 is the preferred solution.

To support iGPU over the Barlow controller, the NVL RVP will support a TCSS module-based solution as shown in the figure below. The miniDP (mDP) will be used on the module. The iGPU over TCP is connected to one of the inputs of the 2:1 MUX retimer, and the second input will be from the dGPU through the miniDP.

The GPIO MUX control from SoC is not supported as of now. Need manual switching on module to change the input.

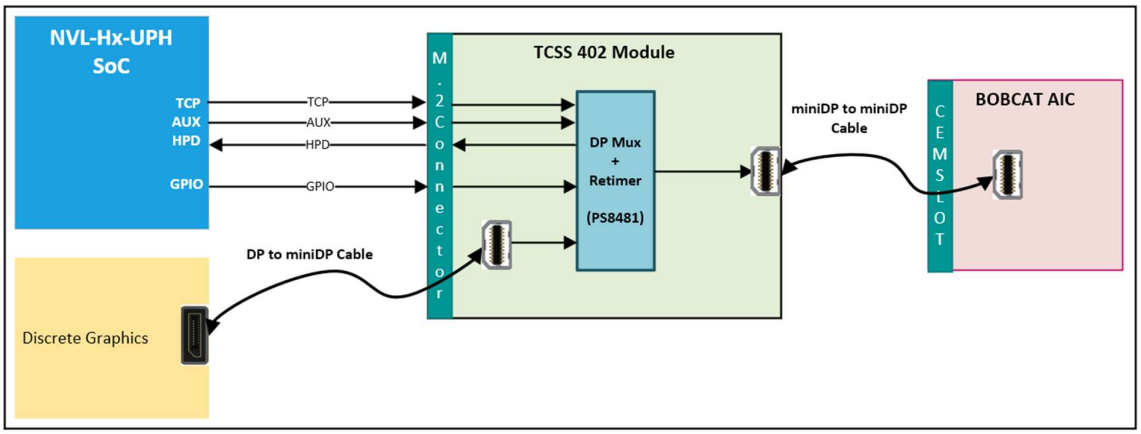


Figure 6-3 : TCSS 402 DP Retimer MUX module for iGPU support

6.11. Download & Execute (DnX) Support

Download & Execute (DNX) is ZBB'd in NVL-AX/AM RVPs.

6.12. Protection Circuit

Specific ESD protection diodes are provided for all the signals close to the Type C port connector. The Type-C connector has a higher pin density than legacy USB connectors. As a result, it is easier to accidentally short VBUS to adjacent pins. With the potential of having VBUS of up to 48 V, it is possible to have a short between the 48V and a 5V line (such as SBU, CC and so on). To protect against this potentially catastrophic event, VBUS short circuit protection is required. Short circuit protection on the SBU and CC lines are taken care in PD add-in card. No additional protector IC is provided on RVP board.

VBUS is also adjacent to the high differential lines, refer to the connector pinout in the Type C specification. These pins are protected using a series Resistor-Capacitor combination between the pins of the Type C connector and the chip. Refer to the Product Design Guide (PDG) document for more accurate details on the same.

6.13. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

7. Imaging – CSI Camera

7.1. Overview

IPU8 is the 8th generation Image Processing Unit (IPU) used in NVL mobile segment. For NVL CSI data and clock lanes originate from SOC. The SOC has 3 CLKOUTs for the camera.

NVL RVP will have two CRD-60 connectors, CRD1 connected with CSI A and B ports and CRD2 with CSI C ports. The NVL PHY supports CSI-2 D PHY v2.1 and CSI-2 C PHY v2.0. The Camera sensors may be connected through CSI-2 over C-PHY or CSI-2 over D-PHY conduit options. Platform allows for a flexible configuration allowing each of the camera modules to use x1, x2, or x4 CSI-2 over D-PHY or T1, T2, T3 (Trios) CSI-2 over C-PHY port.

- NVL AX/AM RVP will be having C-PHY pinout on both CRD connectors (D-PHY over C-PHY support included)

Table 17: Configuration support each NVL RVP

CRD CONNECTOR	NVL AX/AM RVP
CRD Connector 1 (Port A & B)	CSI C-PHY 3T (D-PHY over C-PHY support included)
	No support for AON ULP AIC
CRD Connector 2 (Port C)	CSI C-PHY 2T (D-PHY over C-PHY support included)

NVL will support secure touch camera privacy feature via DIP switch. The DIP switch will be controlled by a GPIO. When secure touch GPIO is HIGH, camera will be masked and when it is LOW, camera will function as normal.

NVL follows the PTL CRD connector placement and routing. The below change done in PTL will be carry forwarded to NVL as well.

Table 18: CSI Port and Connector Mapping with G3 AIC

NVL CRD	CRD G3 (CPHY-DPHY-eUSB) AIC
CRD Conn 1 (Port A & B)	J4 (UF & IR)
CRD Conn 2 (Port C)	J3 (WF)

The camera configurations for NVL are as below. The left side table shows the Mapping supported based on the Silicon pin list. The right-side table shows the mapping possible on RVP.

Table 19: The camera configurations for NVL

IPU input subsystem configuration									RVP Camera support/ configuration							
IPU PHY details		Silicon pin list	DPHY camera mapping			CPHY camera mapping			Package Pin map	DPHY RVP CRD - G1/D1	DPHY RVP CRD - G3	CPHY-DPHY RVP (New CPHY-DPHY CRD -G1/D1)		CPHY-DPHY RVP (New CPHY-DPHY CRD -G3)		
										DPHY mode	DPHY mode	CPHY mode	DPHY mode	DPHY mode	CPHY-DPHY mixed mode	CPHY Mode NOT POR
SNPS CPHY / DPHY combo PHY - A	CPHY/ DPHY Lane aggregation supported b/w PHY A & B	xxcsi_a_dp0_a0	x1 DPHY	x2 DPHY	x4 DPHY	T1 (x1 Trio) CPHY	T2 (x2 Trio) Trio CPHY	T3 (x3 Trio) Trio CPHY	CSI_A_DP0_A0	X1/ x2/ x4 DPHY camera (via 1st CRD)	X1/ x2 DPHY camera	T1/ T2/ T3 CPHY camera (via 1st CRD)	X1/ x2/ x4 DPHY camera (via 1st CRD)	X1/ x2 DPHY camera	X1/ x2 DPHY camera	T1/ T2 CPHY camera
		xxcsi_a_dn0_b0							CSI_A_DN0_B0							
		xxcsi_a_ckp_c0							CSI_A_CKP_C0							
		xxcsi_a_ckn_c1							CSI_A_CKN_C1							
		xxcsi_a_dn1_b1	NC			NC			CSI_A_DN1_B1							
		xxcsi_a_dp1_a1							CSI_A_DP1_A1							
SNPS CPHY / DPHY combo PHY - B		xxcsi_b_dp0_a0	x1 DPHY	x2 DPHY	NC	T1 (x1 Trio) CPHY	T2 (x2 Trio) Trio CPHY	NC	CSI_B_DP0_A0	NC	X1/ x2 DPHY camera (IR)	NC	NC	X1/ x2 DPHY camera (IR)	X1/ x2 DPHY camera (IR)	T1/ T2 CPHY camera
		xxcsi_b_dn0_b0							CSI_B_DN0_B0							
		xxcsi_b_ckp_c0							CSI_B_CKP_C0							
		xxcsi_b_ckn_c1							CSI_B_CKN_C1							
		xxcsi_b_dn1_b1	NC			NC			CSI_B_DN1_B1							
		xxcsi_b_dp1_a1							CSI_B_DP1_A1							
SNPS CPHY / DPHY combo PHY - C	NA	xxcsi_c_dp0_a0	x1 DPHY	x2 DPHY	x2 DPHY	T1 (x1 Trio) CPHY	T2 (x2 Trio) Trio CPHY	T2 (x2 Trio) Trio CPHY	CSI_C_DP0_A0	X1/ x2 DPHY camera (via 2nd CRD)	X1/ x2 DPHY camera	T1/ T2 CPHY camera (via 2nd CRD)	X1/ x2 DPHY camera (via 2nd CRD)	X1/ x2 DPHY camera	T1/ T2 CPHY camera	T1/ T2 CPHY camera
		xxcsi_c_dn0_b0							CSI_C_DN0_B0							
		xxcsi_c_ckp_c0							CSI_C_CKP_C0							
		xxcsi_c_ckn_c1							CSI_C_CKN_C1							
		xxcsi_c_dn1_b1	NC			NC			CSI_C_DN1_B1							
		xxcsi_c_dp1_a1							CSI_C_DP1_A1							

7.1.1. Camera Over eUSB2

NVL is the first silicon to support eUSB2 interfaces. As a result, there will be no legacy USB2.0 pins available on the NVL silicon. For further details, please refer to the section titled “USB 3.2, USB2.0 & eUSB2” in this document.

Eusb2 interfaces can support camera and other native devices such. Several vendors have started designing Eusb2-based camera modules. The NVL Silicon complies with the euSB2 V1 specifications. A new version called Eusb2v2 has been released, but it is not supported here.

NVL RVP offers an option to validate Eusb2 V1 based camera modules through CRD connectors. CRD Connectors provide the capability to validate Eusb2-based cameras.

7.2. Imaging domain platform MRD/PRD

Below is the platform MRD/ PRD for the Imaging domain.

- Platform MRD HSD link.
- Imaging Domain platform PRD HSD link.

7.3. Imaging domain RVP LZ/ PRD

TBD

Table 20: Camera feature support mapping on NVL RVPs

Si#	Domain Feature	Description	NVL-AX/AM
1	**MIPI CSI based camera support**	D-PHY & C-PHY	Yes, CRD Gen2 Conn 1/2 (C PHY and DPHY (DPHY over CPHY routing))
2	**USB2 UF camera Support**	Via Type A/ Type-C USB2 con	Via Type A/ Type-C USB2 con
3	**eUSB2 camera Support**	eUSB2 V1	Yes. CRD Gen2 conn 1 (CPHY/DPHY Conn)
4	**Lid Controller Hub Support**	via AIC on CRD con1	No support
5	**eUSB2 V2 Camera Support**	Yes CRD Gen2 Conn2 (Only for RZL)	No support

7.4. HW BOM

Camera based BOM for NVL RVP are listed below.

Table 21: Camera based BOM for NVL RVP

Si#	HW BOM Description	Part#/ IPN	Vendor	HSD link
1	**WF/UF RGB – 13MP 2D Camera**	OV13B	Omnivision	TBD
2	**RGB-IR: Legacy from previous project**	OV01A1S	Omnivision	TBD
3	**UF IR Camera**	OG0VA1B	Omnivision	TBD
4	**DPHY RGB 8M Low power camera**	OV08X40	Omnivision	TBD
5	**UF Camera USB2**	KBDD741 V2	NA	TBD
6	**UF Camera eUSB2 5.2 MP**	OV05C10(KAFD913)	Omnivision	TBD
7	**CPHY Camera (UF and WF) 14.5MP**	IMX688	Sony	TBD

7.5. AIC List

AIC supported-

- AICs supported in NVL RVP SKUs which is based on CPHY-DPHY based CRD CONN pinout

Please note that AICs supports DPHY-based pinout are not compatible with CPHY-DPHY pinout, and vice versa. Do not interchange these cards.

Below table captures the list of Camera AIC supported on NVL RVP,

Table 22: Below table captures the list of Camera AIC supported on NVL RVP.

CRD CONN AICs	CPHY-DPHY Pinout AX/AM RVP	Transfer Card (X'FER Card)	Camera module/ Module PN#
CRD D1 AIC (DPHY)	No Support	All existing DPHY Xfer card BC-A12 - OV08X40 BCA11 - OG0VA1B BCA1- OV13B BCA10-OV01A1S	OV08X40 - KAFE799 OG0VA1B-KPFA068 OV13B-KBAG152 OV01A1S- KAFB025
CRD G3 AIC (DPHY)			
CRD D1 CPHY DPHY with eUSB2	Yes, New AIC	<u>New CPHY xfer card</u> BCA21 <u>New DPHY xfer card</u> BC-A20 - OV08X40 BCA18 - OV01A1S BCA22- OG0VA1B BCA19 - OV13B <u>New Eusb2 xfer card</u> BC-eU3	<u>CPHY Modules</u> IMX688 -KBFG809 <u>DPHY Modules</u> OV08X40-KAFE799, OV01A1S-KAFB025 OG0VA1B-KPFA068 OV13B-KBAG152 <u>Eusb2 Modules</u> Realtek EVB + OV05C10 -KAFD913 +OG0VA1B-KPFA068
CRD G3 CPHY DPHY			

CRD CONN AICs	CPHY-DPHY Pinout AX/AM RVP	Camera module/ Module PN#
Synaptics Sabre AIC	Not Supported	TBD

7.6. High level Block diagram

Below given is the high-level block diagram of imaging circuit implementation in NVL RVP.

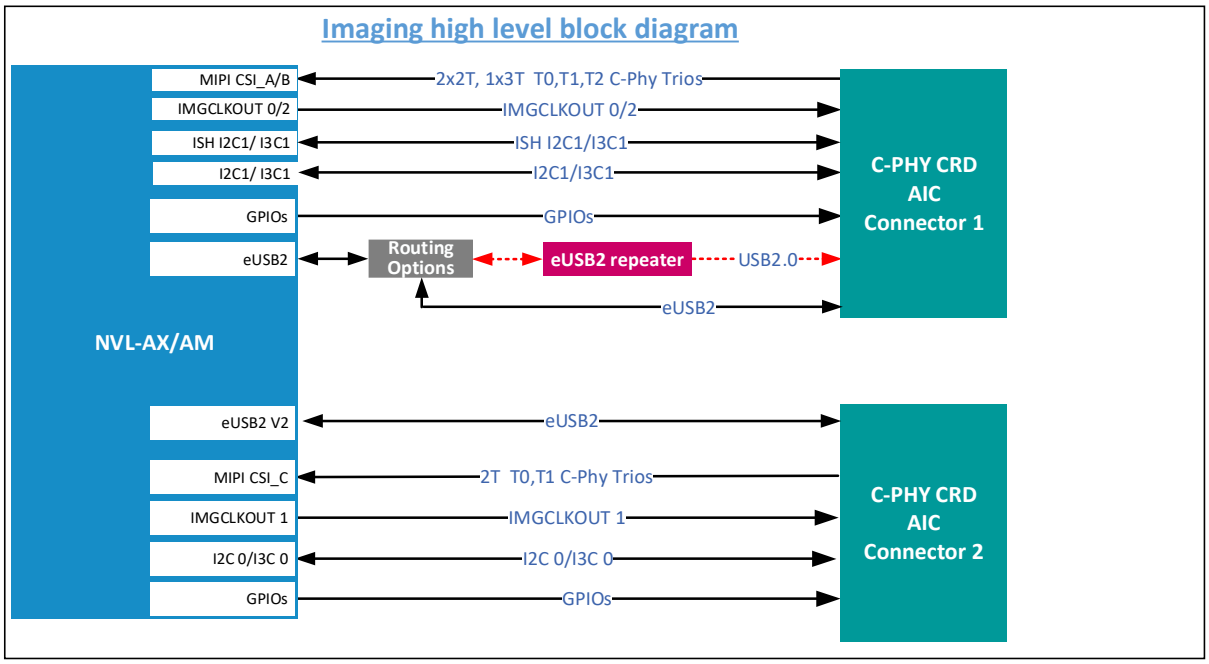


Figure 7-1: NVL CSI C-PHY imaging support high level block diagram

7.7. CRD- 60 Connector Pinout

The CRD connector pinout for CPHY can be found in below RVP Wiki link.

https://wiki.ith.intel.com/display/ITSDesignWiki/Camera

8. Clocks

8.1. Overview

In NVL SOC, the PCH-S pairs with NVL PCD-H in a different PCH mode called “PCH.IOE” mode. The chipset has 2 major clock sources. All the sub-system clocks and external clock outputs are derived though internal PLLs. The two major clock sources for NVL mobile clocking are:

1. 38.4 MHz crystal.
2. 32.768 kHz crystal for RTC.

8.2. Clock domain platform MRD/PRD

Below are the platform MRD/ PRD for the HSIO domain.

- Platform MRD HSD link.
- PRD for clock domain PRD HSD link.
- RVP PRD -TBD

8.3. NVL Clock specification

8.3.1. 38.4 MHz Crystal

Below are the 38.4 MHz crystal requirements for the NVL PCD.

Table 23: 38.4 MHz crystal requirements

Specification	Value	Notes
Nominal Frequency (F0)	38.4 MHz	Fundamental Overtone
Mode of Oscillation	AT Cut-Fundamental	
C_L	10 pF	Crystal Load Capacitance
Crystal Calibration Tolerance	±20 ppm Max	At 25C. This may be relaxed if the overall platform crystal ppm is relaxed.
Operating Temperature Range	- 40 to + 85°C	
Crystal Frequency Stability over Temp range	±20 ppm Max	This may be relaxed if the overall platform crystal ppm is relaxed.
Typical operating drive level	100 uW	
Maximum operating drive level	300 uW	
Equivalent Series Resistance	30 ohms max	
Shunt Capacitance	3 pf	
Aging at 25 C	±10 ppm	Max over 10 years.
R_F	200 kΩ	
Discrete Board Caps	15 (+/- 5%) pf	

8.3.2. 32.768 kHz Crystal

Below are crystal specifications for the 32.768 KHz crystal supporting the PCD.

Table 24: 32.768 KHz crystal requirement

Specification	Value	Notes
Nominal Frequency (F0)	32.768 kHz	Fundamental Overtone
Calibration Tolerance	±20 ppm Max	+25°C, Not include aging
Crystal Frequency Stability over Temp range	±20 ppm Max	
Turning Point	+25 ±5°C	
Aging	±10 ppm Max. / 10 year	+25 °C
ESR	50 kΩ Max. 40 kΩ typ	
C_L	12.5 pF	
Operating Temperature range	- 40 to + 85°C	

PCH can be made to work as an IO expander mode on a NVL mobile platform. The implementation is to forward the RTC (32.768KHz) and XTAL 38.4MHz from PCD die to PCH.IOE differentially. In the PCH these 2 clocks as received by the differential input buffer. 38.4MHz XTAL will follow a similar clkreq/clkack handshake between the PCD and PCH. In the PCH.IOE mode the roles are reversed when compared with PCH mode. PCH.IOE die will initiate the clock request to PCD and the PCD will respond with the clock and the clock ack. This handshaking will happen over eSPI using virtual wire messaging like the desktop implementation. For details on the virtual wire messaging refer to below link.

Reference**:**

NVL PCH-S - PCD/PCH Interface:
https://docs.intel.com/documents/pch_doc/NVL/PCH/HAS/PCH_Interface_HAS/PCH_Interface_HAS.html#virtual-wire-interface

NVL PCH Integrated System Clock:
https://docs.intel.com/documents/pch_doc/NVL/PCH/HAS/Chap38_NVL_PCH_Integrated_System_Clock/Chap38_NVL_PCH_Integrated_System_Clock.html#pch.ioe-mode

NVL PCD H System Clock Domains:
https://docs.intel.com/documents/pch_doc/NVL/PCD-H/HAS/Chap05_NVL_PCD_H_Clock_Domains/Chap05_NVL_PCD_H_Clock_Domains.html

NVL Platform Clocking:
https://docs.intel.com/documents/ClientPlatform/Domains/Clocking/nvl/NVL_Clocking_PAS.html#platform-requirements

8.3.3. NVL Clock signals

Below are the input clocks to PCD-H die on NVL RVP.

Table 25: PCD-H Clock Inputs on NVL

Signal Name	Description
RTCX1/ RTCX2	32.768KHz crystal input for Real time clock
Single ended Crystal RTCX1	Single-ended RTC crystal input by driving 32.768Khz CMOS clock on RTCX1 [Not used on RVP]
XTAL_IN/OUT	38.4MHz crystal input for iSCLK (integrated System Clock) block
CRF_CLKREQ	To be sent to iSCLK & CRF Quasar to Synchronize CRF & Quasar
SRCCLKREQB [8:0]	SRCCLKREQB is used to support clock request protocol to enable or disable SRC clocks distribution to off-chip. In addition, the SRCCLKREQB is also used for PCIe power management (L1.off, etc.).
OBS[1:0]MON_ISCLK	iSCLK monitoring pins for debug usage
SOC_REFRCOMP_ISCLK	Connected to an external precision resistor for Differential buffer, RCOMP between VSS and this pad.
xxpcd_bgr_isclk	ISCLK bandgap requires a bump that is driven by tester during sort and class for BG trimming.

Below are the output clocks from PCD-H die in NVL RVP.

Table 26: PCD-H Clock output on NVL

Signal Name	Frequency & SSC Support	Description
SUSCLK	32.768KHz without SSC	Suspend clock that generated from the RTC crystal oscillator
CLKOUT_SOC_[0:8]_N/P	100MHz - Gen5 Capable with SSC	100MHz differential source clock for external PCIe Device.
IMGCLKOUT [0:2]	19.2 MHz	Clock for external camera sensor, from is CLK Main PLL (low power PLL)
xtal_out_38_p/n	38.4MHz	IsCLK 38.4MHz output port for PCH.IOE usage.

Below are the Input clocks for PCH-S die in NVL RVP.

Table 27: PCH-S Clock Inputs on NVL

Signal Name	Description
XTAL_IN/OUT	32.768KHz crystal input for Real time clock. In PCH IOE mode this input is sourced from SUSCLK of PCD-H.
CLKIN_XTAL_P/N	38.4MHz clock input for iSCLK (integrated System Clock) block from PDC-H.
SRCCLKREQB [11:0]	SRCCLKREQB is used to support clock request protocol to enable or disable SRC clocks distribution to off-chip
CRF_CLKREQ	To be sent to iSCLK & CRF Quasar to Synchronize CRF & Quasar
DMI_REFCLKP/N	DMI Reference clock.

Below are the output clocks from PCH-S die in NVL RVP.

Table 28: PCH-S Clock output on NVL

Signal Name	Frequency	Description
CLKOUT_PCH_SR [0:11]	100MHz	100 MHz Differential reference clocks for PCI Express devices. SRCCLK [3:0] are Gen4 capable and SRCCLK [11:4] are Gen5 capable.

MFIT INFO TBD (will update in HAS1.0 version).

By default, CLKREQ will be enabled as Native GPIO function. To use these pins as a CLKREQ it needs to be mapped in the BIOS.

The Gbe LAN PHY needs 25MHz input which will be fed from an external crystal input. The Embedded controller has the external 32.768kHz crystal input as the default option along with SUS_CLK option driven from SOC. Any other interface specific clocks required for third party devices will be derived out of the external crystals specific to the device requirements.

8.4. NVL RVP: SRC Clock and CLK REQ Mapping

Clock and Clock request mapping for PCD-H on NVL RVP is listed below.

Table 29: Clock and Clock request port mapping for PCD-H across RVP SKUs (TBD)

Clock	NVL-AX/AM RVP
Gen5 SRC CLK &CLKREQ #0	x4 DMI (PCIe Gen5)
Gen5 SRC CLK &CLKREQ #1	X4 PCIe Gen4 CEM Slot #2 (x2 Mode)
Gen5 SRC CLK &CLKREQ #2	M.2 WLAN Key E
Gen5 SRC CLK &CLKREQ #3	TBD
Gen5 SRC CLK &CLKREQ #4	x4 PCIe Gen4 B(0-3) CEM Slot #3 dTBT Barlo Ridge #1
Gen5 SRC CLK &CLKREQ #5	Gbe LAN Support
Gen5 SRC CLK &CLKREQ #6	x8 PCIe Gen5 CEM Slot #1
Gen5 SRC CLK &CLKREQ #7	M.2 NVMe SSD #1 (x4 PCIe Gen5)
Gen5 SRC CLK &CLKREQ #8/ UFS REF Clock	MCIO (TBD)

Clock and Clock request mapping for PCH-S on NVL RVP is listed below.

Table 30: Clock and Clock request port mapping for PCH-S across NVL RVP SKUs

CLK	NVL-AX/AM RVP
Gen4 SRC CLK &CLKREQ #0	NC (No connect pin in RVP)
Gen4 SRC CLK &CLKREQ #1	NC (No connect pin in RVP)

Gen4 SRC CLK &CLKREQ #2	NC (No connect pin in RVP)
Gen4 SRC CLK &CLKREQ #3	NC (No connect pin in RVP)
Gen5 SRC CLK &CLKREQ #4	M.2 NVMe SSD #2 (x4 PCIe Gen5)
Gen5 SRC CLK &CLKREQ #5	M.2 NVMe SSD #3 (x4 PCIe Gen5)
Gen5 SRC CLK &CLKREQ #6	M.2 NVMe SSD #4 (x4 PCIe Gen5)
Gen5 SRC CLK &CLKREQ #7	NC (No connect pin in RVP)
Gen5 SRC CLK &CLKREQ #8	NC (No connect pin in RVP)
Gen5 SRC CLK &CLKREQ #9	NC (No connect pin in RVP)
Gen5 SRC CLK &CLKREQ #10	NC (No connect pin in RVP)
Gen5 SRC CLK &CLKREQ #11	NC (No connect pin in RVP)

8.5. NVL Clock mapping Block Diagram

Below image depicts the Clock mapping for NVL RVPs.

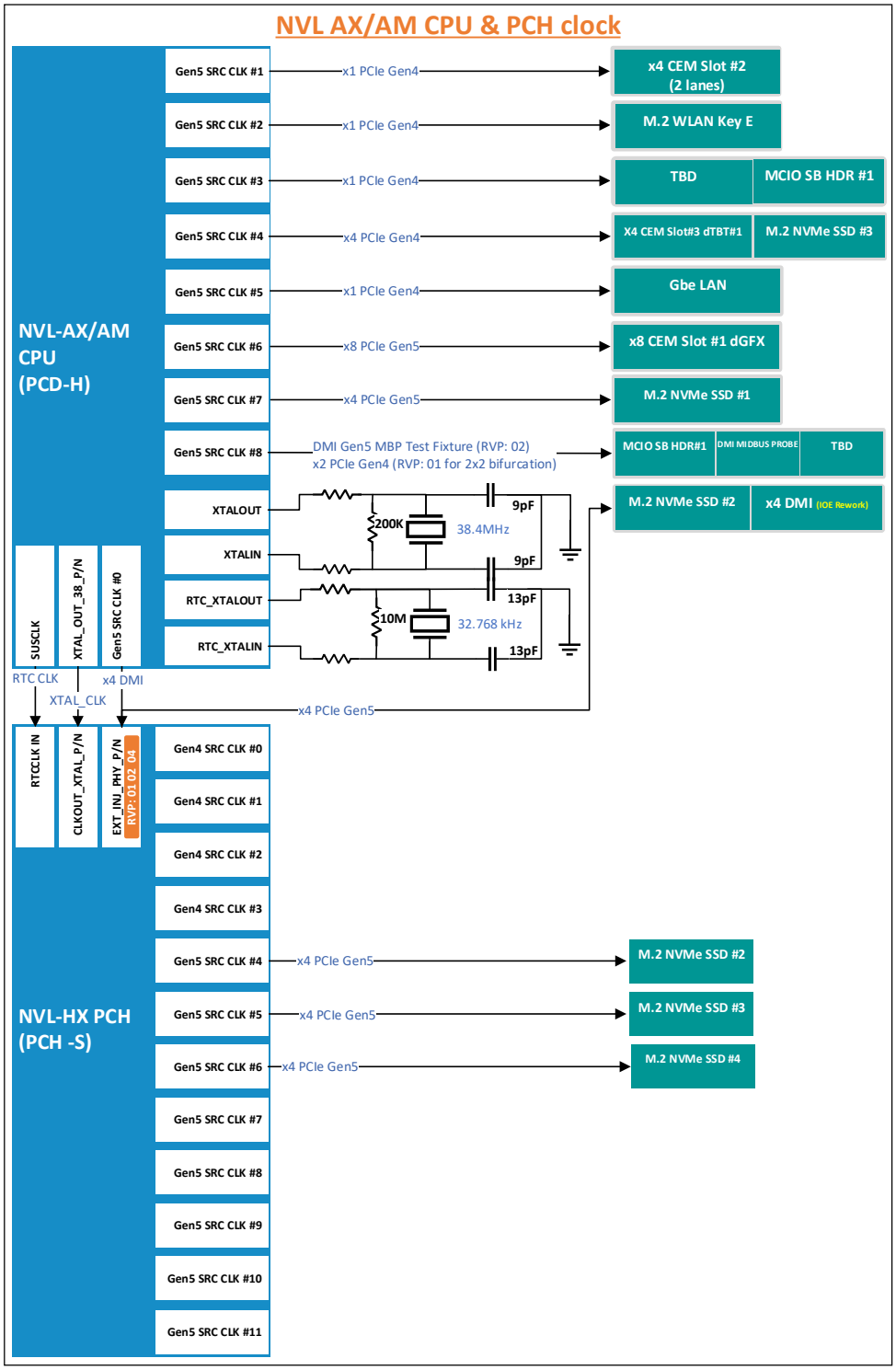


Figure 8-1: Clock and Clock request mapping for NVL RVP

9. HSIO

9.1. Overview

NVL-AX/AM platform supports various HSIO interfaces like PCIe Gen5/Gen4, USB 3.2 Gen2, Gbe LAN to connect different peripheral devices from NVL SOC and PCH-S Die (PCH -IOE).

9.1.1. NVL Platform HSIO support details

NVL PCD die supports:

1. 2 USB3.2 Gen2 ports
2. 8 eUSB2 ports.
3. 2 x4 PCIe Gen4 lanes. 1 of these lanes is muxed with Gbe interface.
4. 1x8 and 2x4 PCIe Gen5 lanes. 1 of the x4 lanes is muxed with DMI interface.

NVL PCH (PCH -S) die supports:

1. 10 USB3.2 Gen2 ports.
2. 3x4 PCIe Gen4 lanes.
3. 3x4 PCIe Gen5 lanes.
5. 1x4 PCIe Gen5 based DMI interface.

9.1.2. PCIe device support on NVL-AX/AM RVP

1. 2x M.2 Key-M SSD Gen4/ Gen5 – Without PCH IOE (with PCH IOE 4x M.2 Key-M SSD Gen4/ Gen5)
2. M.2 Key-E WLAN
3. Integrated Gbe LAN
4. Barlow Ridge discrete TBT controller (Through AIC)
5. x8 PCIe Gen5 DT Slot (Open ended) – for discrete GFx
6. x4 PCIe Gen4 DT Slot (Open ended) – for various FV test.
7. x4 PCIe DT Slot -2 Lanes only (Open ended) – for SD 7.0 AIC, Foxville discrete LAN AIC etc

9.2. HSIO domain platform MRD/PRD

Below are the platform MRD/ PRD for the HSIO domain.

- Platform MRD HSD link.
- PRD for PCIe domain PRD HSD link.
- PRD for Graphics domain PRD HSD link.

9.3. HSIO Features Supported (RVP LZ/ PRD)

9.3.1. RVP PRD

TBD

9.3.2. Feature support for HSIO

Below table shows HSIO feature supported on NVL RVPs.

Table 31: PCD-H HSIO feature support mapping on NVL RVPs

PCIe Lane #	RVP-01
	NVL-AX/AM
PCIe Gen4 A0/ Gbe LAN	Gbe LAN Support

PCIe Gen4 A1/ Gbe LAN	M.2 WLAN Key E
PCIE Gen4 A2	X4 PCIe Gen4 CEM Slot #2 (2 lanes only)
PCIe Gen4 A3	
PCIe Gen4 B0	x4 PCIe Gen4 CEM Slot #3 dTBT Barlo Ridge #1
PCIe Gen4 B1	
PCIe Gen4 B2	
PCIe Gen4 B3	
DMI/ PCIe Gen5 C0	x4 DMI (PCIe Gen5)/M.2 NVMe SSD #4 (rework - from PCD-H PCIe gen5 and PCH.IOE PCIe gen5 DMI)
DMI/ PCIe Gen5 C1	
DMI/ PCIe Gen5 C2	
DMI/ PCIe Gen5 C3	
PCIe Gen5 D0	x8 PCIe Gen5 CEM Slot #1
PCIe Gen5 D1	
PCIe Gen5 D2	
PCIe Gen5 D3	
PCIe Gen5 D4	
PCIe Gen5 D5	
PCIe Gen5 D6	
PCIe Gen5 D7	
PCIe Gen5 E0	M.2 NVMe SSD #1 (x4 PCIe Gen5) w /I2C for NIST
PCIe Gen5 E1	
PCIe Gen5 E2	
PCIe Gen5 E3	

Table 32: PCH-S HSIO feature support mapping on NVL RVPs

PCIe Lane #	NVL AX/AM RVP
PCIE Gen4 A0	NC (No connect pin in RVP)
PCIE Gen4 A1	
PCIE Gen4 A2/ Gbe LAN	
PCIE Gen4 A3	
PCIE Gen4 B0/ SATA 0	NC (No connect pin in RVP)
PCIE Gen4 B1/ SATA 1	
PCIE Gen4 B2/ SATA 2/ Gbe LAN	
PCIE Gen4 B3/ SATA 3	
PCIE Gen4 C0/ SATA 4	NC (No connect pin in RVP)
PCIE Gen4 C1/ SATA 5	
PCIE Gen4 C2/ SATA 6/ Gbe LAN	
PCIE Gen4 C3/ SATA 7	
PCIE Gen5 D0	M.2 NVMe SSD #3 (x4 PCIe Gen5)
PCIE Gen5 D1	

PCIE Gen5 D2	
PCIE Gen5 D3	
PCIE Gen5 E0	M.2 NVMe SSD #2 (x4 PCIe Gen5)
PCIE Gen5 E1	
PCIE Gen5 E2	
PCIE Gen5 E3	
PCIE Gen5 F0	M.2 NVMe SSD #4 (x4 PCIe Gen5)
PCIE Gen5 F1	
PCIE Gen5 F2	
PCIE Gen5 F3	
DMI_0 (PCIe Gen5)	x4 DMI (PCIe Gen5)
DMI_1 (PCIe Gen5)	
DMI_2 (PCIe Gen5)	
DMI_3 (PCIe Gen5)	

9.4. HSIO configurations in NVL RVP's

Based on the platform LZ, POR & platform requirement initial HSIO Mapping has been done for NVL Platform. RVP ModPHY Mapping table will be used by the soft strap team & BIOS team to configure the individual lane as per RVP recommendation. RVP Implementation will support multiple configurations by sharing the same lanes for different function. Board rework and IFWI changes will be required to enable the shared feature which has different function. Refer below links for configuration supported by PCD-H and PCH-S.

NVL HSIO HAS: https://docs.intel.com/documents/pch_doc/NVL/PCD-S/HAS/HSIO/NVL_HSIO_HAS.html

NVL PCH HSIO HAS: https://docs.intel.com/documents/pch_doc/NVL/PCD-S/HAS/HSIO/NVL_PCH_HSIO_HAS.html#src-clock

Below table captures the HSIO configuration supported on NVL RVP with respect to PCD-H CPU.

Table 33: HSIO support by NVL PCD-H on NVL RVP

Die	Controller	PHY	Port #	PCIe	PCIe Port Configs			AX/AM
					x4	x2	x1	
PCD-H	XHCI (USB3)	USB3 (SNPS)	USB32_1					Yes
			USB32_2					
	PXPA Gen4 (4px4, 2VC)	MP1 (SNPS) PCD MP, x4	PCIe_A0	Yes		x2	x1	Yes
			PCIe_A1	Yes			x1	
			PCIe_A2	Yes		x2	x1	
			PCIe_A3	Yes			x1	
	PXPB Gen4 (4px4, 2VC)	MP2 (SNPS) PCD MP, x4	PCIe_B0	Yes	x4	x2	x1	Yes
			PCIe_B1	Yes			x1	
			PCIe_B2	Yes		x2	x1	
			PCIe_B3	Yes			x1	
	PXPC Gen5 (DMI) (2px4, 2VC)	P3 (IPG HSPHY) Gen5, x4	PCIe_C0	Yes	x4	x2		Yes
			PCIe_C1	Yes				
			PCIe_C2	Yes		x2		
			PCIe_C3	Yes				
	PXPD Gen5 (2px8, 2VC)	P4 (IPG HSPHY Gen5, x8	PCIe_D0	Yes	x8	x4		Yes
			PCIe_D1	Yes				
			PCIe_D2	Yes				
			PCIe_D3	Yes				
			PCIe_D4	Yes		x4		

		PCIe_D5	Yes				
		PCIe_D6	Yes				
		PCIe_D7	Yes				
PXPE Gen5 (2px4, 2VC)	P5 (IPG HSPHY) Gen5, x4	PCIe_E0	Yes	x4	x2		Yes
		PCIe_E1	Yes				
		PCIe_E2	Yes		x2		
		PCIe_E3	Yes				

Below table captures the HSIO configuration supported on NVL RVP with respect to PCH-S PCH.

Table 34: HSIO support by NVL PCH-S on NVL RVP

PCH-S HSIO configuration on RVP								
Die	Controller	PHY	Port #	PCIe	PCIe Port Configs			USB 3.2 10G
					x4	x2	x1	
PCH-S	PXPA (Gen4 4px4)	MP1 PCH MP, x4	PCIe_A0	Yes	x4			
			PCIe_A1	Yes				
			PCIe_A2	Yes				
			PCIe_A3	Yes				
	PXPB (Gen4 4px4)	MP2 PCH MP, x4	PCIe_B0_SATA0	Yes	x4			
			PCIe_B1_SATA1	Yes				
			PCIe_B2_SATA2	Yes				
			PCIe_B3_SATA3	Yes				
	PXPC (Gen4 4px4)	MP3 PCH MP, x4	PCIe_C0_SATA4	Yes	x4			
			PCIe_C1_SATA5	Yes				
			PCIe_C2_SATA6	Yes				
			PCIe_C3_SATA7	Yes				
	PXPD (Gen5, 2px4)	P1 PCH Gen5, x4	PCIe_D0	Yes	x4			
			PCIe_D1	Yes				
			PCIe_D2	Yes				
			PCIe_D3	Yes				
	PXPE (Gen5 2px4) PXPEx (Gen5 2px4)	P2 PCH Gen5, x4	PCIe_E0	Yes	x4			
			PCIe_E1	Yes				
			PCIe_E2	Yes				
			PCIe_E3	Yes				
	PXPE (Gen5 2px4) PXPEx (Gen5 2px4)	P3 PCH Gen5, x4	PCIe_F0	Yes	x4			
			PCIe_F1	Yes				
			PCIe_F2	Yes				
			PCIe_F3	Yes				
	DMI (Gen5 1px4)	P0 PCH Gen5, x4	DMI_0	Yes	x4			
			DMI_1	Yes				
			DMI_2	Yes				
			DMI_3	Yes				
	XHCI (USB3)	U1, PCH USB3, x4						Yes
		U2, PCH USB3, x2						Yes
		U3, PCH USB3, x4						Yes
	XHCI (USB2)	USB2 PHY 2x7						Yes

9.5. AIC List

HSIO based AICs used on NVL RVP is listed below.

Table 35: HSIO based AICs used on NVL RVP

Si#	HW BOM Description	Part#/ IPN	Vendor	HSD link
1	**PCIe Gen5 mobile GFx card with DP UHBR20 support**	TBD	TBD	
2	**PCIe Gen5 desktop GFx card with DP UHBR20 support**	TBD	TBD	
3	**PCIe Gen4 desktop GFx card**	NVDIA	ADA RTX4000	
4	**PCIe Gen4 desktop GFx card**	AMD	NAVI33	
6	**Race point beach AIC**	M30674-006	Intel	
7	**DMI Gen 4 Mid Bus Probe Interposer**	TBD	Intel	
8	**DMI Gen 5 Mid Bus Probe Interposer**	TBD	Intel	

9.6. NVL RVP PCIe Mapping Block diagram

Below block diagrams captures the PCIe mapping on NVL RVPs.

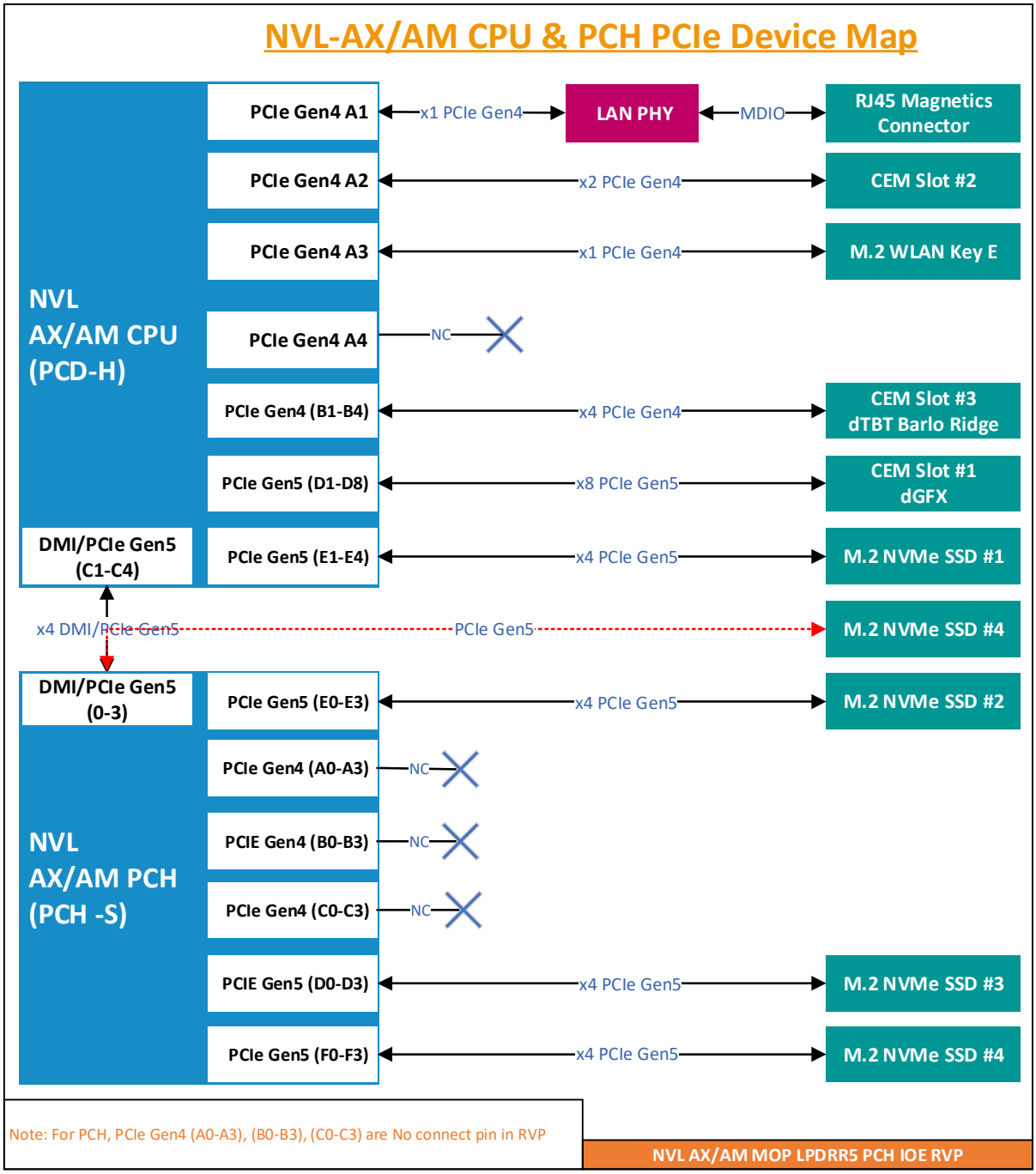


Figure 9-1: NVL-AX/AM CPU & PCH PCIE Device Mapping

9.7. Direct Media Interface (DMI)

In NVL for Direct media interface, DMI3 is adopted like MTL. Major difference here is x8 DMI3 is changed to x4 DMI3 (Gen5 x4 PCIe). NVL, the PCH-S pairs with NVL PCD-H in a different PCH mode called “PCH.IOE” mode. PCH IOE refers to Platform Controller Hub I/O Expansion. PCH.IOE mode provides I/O expansion without most other capabilities present in the PCH, e.g. no manageability. PCD-H die connected to PCH.IOE through DMI Gen5 x4 and eSPI. PCD-H provide xtal clock and RTC clock based on request from PCH.IOE. There are Virtual Wire (VW) messaging between the PCH and PCD-H to support the 4-way XTAL clkreq/clkack handshake. For identifying PCD that is connected to the Hub die, IOC defines a new Fuse bit. In PCH.IOE mode the XTAL and the RTC clocks to the PCH originate from PCD. The DMI clocks is generated from the PCD-H to satisfy the common clocking requirements. The table details the clock related signals between the PCH-S and the PCD-H dies.

Table 36: Clock signals between PCD and PCH on NVL RVP

Clock	PCD-H Name	PCD-H Dir	PCH Name	PCH Dir	Comments
XTAL	XTAL_OUT (GPIO)	output	XTAL_IN (iSCLK)	Input	Single ended 38.4MHz clk
RTC	SUSCLK	output	RTCX1	Input	Single ended 32KHz clk
DMI	CLKOUT_SRC_P [*]	output	EXT_INJ_PHY_P_PAD	input	Any one of the 9 SRC buffers can me mapped to the DMI
	CLKOUT_SRC_N [*]	output	EXT_INJ_PHY_N_PAD	input	
	SRC_CLKREQ# [*]	I/O	DMI_CLKREQB	I/O	Any one of the CLKREQB can be mapped

In NVL DMI is mux with PCIe Gen5 x4. Below image depicts the DMI implementation on NVL RVP.

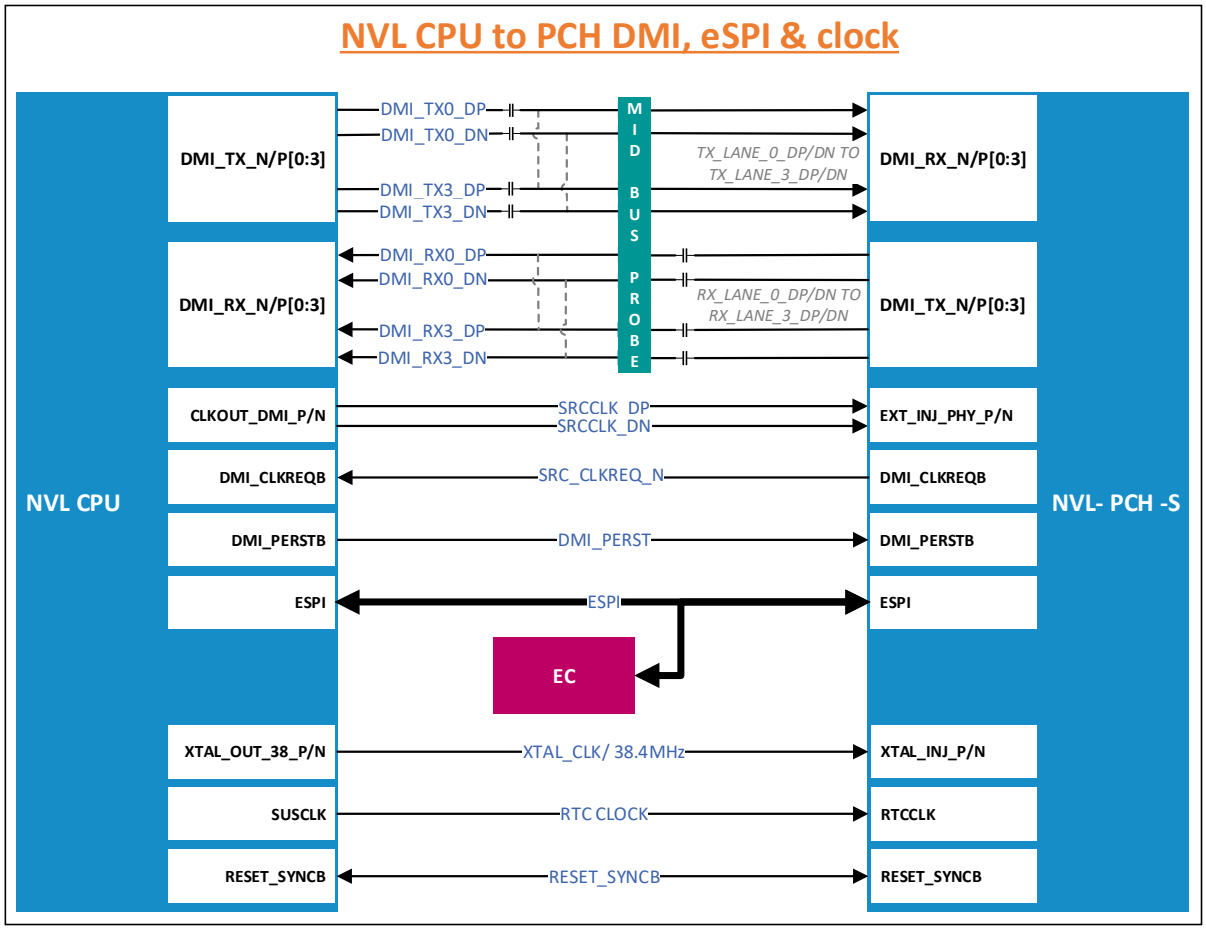


Figure 9-2: DMI implementation on NVL AX/AM RVP with PCH IOE mode

Reference:
https://docs.intel.com/documents/pch_doc/nvl/PCH/HAS/PCH_Interface_HAS/PCH_Interface_HAS.html#introduction

9.8. MCIO Interface (TBD)

MCIO implementation TBD

Figure 9-3: MCIO implementation on NVL RVP

9.9. AIC descriptions

PCH IOE Supported on Mother board. AIC is not supported.

9.9.1. Race Point Beach AIC (TBD)

For MCIO related FE validation, Race point Beach AIC will be used. It is a Validation test card to exercise PCIe Gen5/CXL1.1/CXL2.0 protocols using an FM85 B0 step. MCIO is not PoR for NVL RVP.

Reference: https://wiki.ith.intel.com/pages/viewpage.action?spaceKey=PEVH&title=RACE+POINT+BEACH

9.10. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

10. Storage

10.1. Overview

NVL supports different storage options whose high-level block diagram & details are mentioned in following sections. Below table list the storage interfaces supported by NVL RVP.

Table 37: Storage options supported on NVL RVP

Sl. No	Interface	NVL RVP
1	**PCIe NAND SSD**	Share same M.2 2280 connector interfaced Modules
2	**SD CARD over PCIe**	Realtek RTS5264 SD Card reader (Through PCIex1 slot)

10.2. Storage domain platform MRD/PRD

Below are the platform MRD/ PRD for the storage domain.

- Platform MRD HSD link.
- PRD for storage domain PRD HSD link.

10.3. Storage Features Supported (RVP LZ/ PRD)

Storage domain feature support, Landing Zone and RVP PRD are captured in below section.

10.3.1. RVP PRD

TBD

10.3.2. RVP Landing Zone for HSIO

Below is RVP LZ for storage.

Table 38: RVP LZ for storage

Si#	Domain Feature	Des/ Comments	NVL-AX/AM
1	**M.2 NVMe SSD Gen5**	x4/ x2 config	2x M.2 NVMe SSD Gen5 (from SOC) in PCH-less configuration, but only 1 when SoC is paired with PCH.IOE 3x M.2 NVMe SSD Gen5 (from PCH IOE)
2	**M.2 NVMe Gen4 SSD**	x4/ x2 config	Supported
3	**M.2 SATA SSD**	Not POR for Mobile segment	NA - NOT POR
4	**SATA HDD direct connect**	Not POR for Mobile segment	NA - NOT POR
5	**SATA HDD cable connect**	Not POR for Mobile segment	NA - NOT POR
6	**UFS 4 Gear 5 via (UFS M.2 module)**	POR for Mobile U segment only	NA - NOT POR
7	**UFS 4 Gear 5 w/ redriver via (UFS M.2 module)**	POR for Mobile U segment only	NA - NOT POR
8	**SD card 7.0**	Via PCIe AIC	Supported
9	**SATA Flex (internal cabling)**	Not POR for Mobile segment	NA - NOT POR
10	**SATA ODD**	Not POR for Mobile segment	NA - NOT POR
11	**PLN**		Yes
12	**Platform firmware recovery (NIST 800-193)**		Yes

10.4. NVL RVP: Storage Mapping block diagram

Below block diagram shows the mapping of storage supported by NVL RVP.

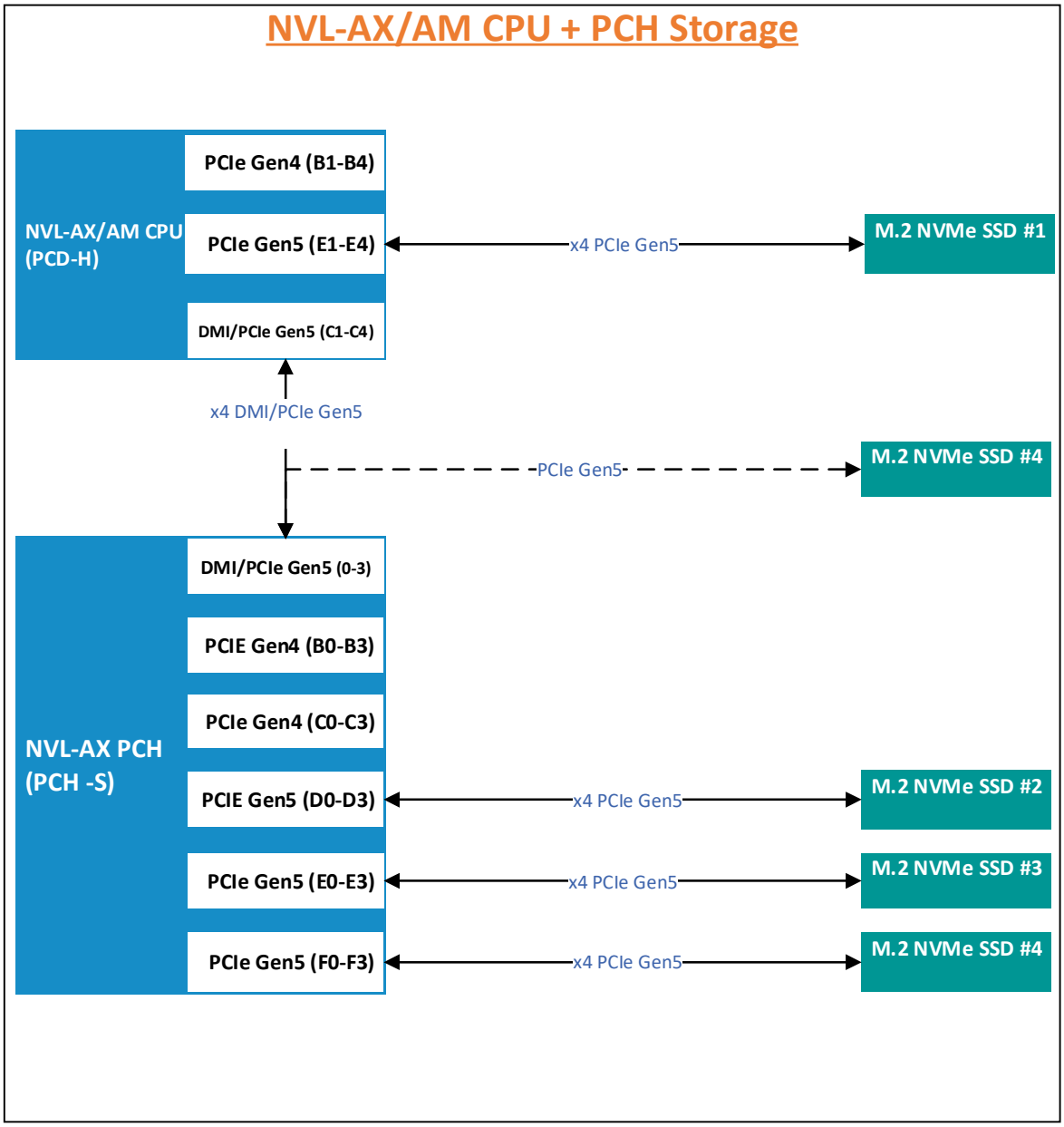


Figure 10-1: NVL-AX + PCH RVP Storage mapping

10.5. HW BOM

Storage based BOM used on NVL RVP are listed below.

Table 39: Storage based BOM used on NVL RVP

Si#	AIC Title	VENDOR	PART NO/ IPN	Link
1	PCIe Gen5 NVMe SSD - Performance - 12-14GB/S @ 11W	Samsung	PM9E1	TBD
2	PCIe Gen5 NVMe SSD - Performance - 12-14GB/S @ 11W	SK Hynix	PCB01	-
3	PCIe Gen5 NVMe SSD - Mainstream - 9-10GB/s @7-8W	-	No Mainstream models on Gen5 SSDs	-
4	PCIe Gen4 NVMe SSD - Performance - 7.5GB/s @8W	WD	SN8000S	TBD
5	PCIe Gen4 NVMe SSD - Performance - 7.5GB/s @8W	Micron	Micron 3500	TBD
6	PCIe Gen4 NVMe SSD - Performance - 7.5GB/s @8W	Samsung	PM9C1b	TBD
7	PCIe Gen4 NVMe SSD - Performance - 7.5GB/s @8W	Kioxia	XG8	TBD
8	PCIe Gen4 NVMe SSD - Performance - 7.5GB/s @8W	SK Hynix	PC811	TBD
9	PCIe Gen4 NVMe SSD - Mainstream - 4-5GB/s @5W	Micron	Micron 2650	TBD
10	PCIe Gen4 NVMe SSD - Mainstream - 4-5GB/s @5W	WD	SN7100S	TBD
11	PCIe Gen4 NVMe SSD - Mainstream - 4-5GB/s @5W	Samsung	PM9C1	TBD
12	NVMe SSD w/ I3C NIST support (Gen4)	WD	SN8000S	TBD
13	NVMe SSD w/ I3C NIST support (Gen4)	Micron	Micron 3500	TBD
14	NVMe SSD w/ I3C NIST support (Gen5)	Samsung	PM9E1	TBD

10.6. AIC List

Storage based AICs used on NVL RVP is listed below.

Table 40: Storage based AICs used on NVL RVP

Si#	Add In Card (AIC) Description	VENDOR	PART NO/ IPN	Wiki link
1	SD Express AIC based on Realtek RTS5264	Realtek	RTS5264	TBD

10.7. M.2 Key-M Connector

NVL-AX/AM RVPs support M.2 SSD Key-M connectors following the PCI SIG M.2 spec. All the M.2 Key-M SSD ports will have RTD3 capability for PERST & WAKE signal coming from SOC.

Below image shows Gen5 NVMe implementation for PCD-H with NIST recovery. Similar implementation will be followed for Gen4 and PCH.IOE based implementation.

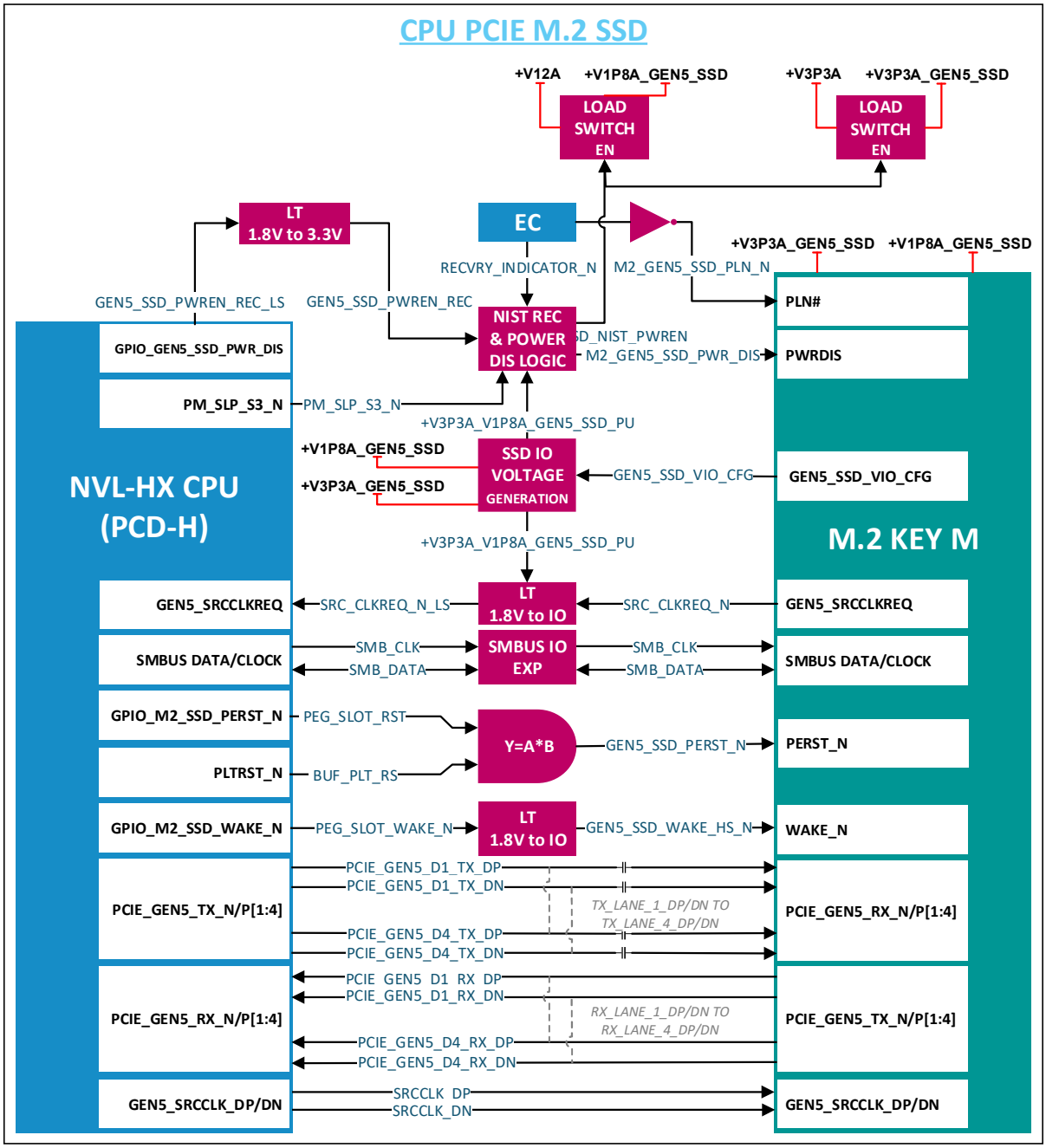


Figure 10-2: M.2 NVME Implementation on NVL AX/AM RVP (BD TBD)

10.7.1. Dynamic M.2 Key-M SSD sideband GPIO voltage level switching (3.3V vs 1.8V)

NVL platform supports 1.8V IO level only. Platforms need level shifter to support legacy M.2 SSD modules with 3.3V sideband GPIO signaling. Upcoming M.2 modules are coming up with two configurations:

- Support both 1.8V/3.3V sideband GPIO signal level
- Support only 1.8V sideband GPIO signal level

For supporting both legacy & upcoming SSD modules, we need dynamic switching of sideband GPIO voltage level between 3.3V & 1.8V.

NVL RVP supports dynamic M.2 Key-M SSD sideband GPIO voltage level (3.3V vs 1.8V) switching.

VIO_CFG is a signal indicates to the Platform that the Adapter supports an independent IO voltage domain for the sideband signals. It is output signal from M.2 Module. Sideband signaling is 3.3V when VIO_CFG signals is low and NC when sideband signaling is 1.8V.

10.7.2. Power Loss Notification (PLN) Support

A sudden loss of power can cause an SSD to lose user data in its volatile write cache & the 3 primary cause for power loss are:

- User presses & holds power button for more than power button overrise time (4s/ 10s/ Custom)
- Battery disconnected in case of notebooks & AC power loss in case of DT systems without UPS.
- Battery runs down.

This proposal will address first cause, the user turning off the power without going through the Windows shut-down process. It is proposed to connect Power Button signal passing through an Open Drain Buffer to M.2 SSD connector Pin 8 & a GPIO from EC to the same open drain buffer. This implementation will be on NVL RVPs.

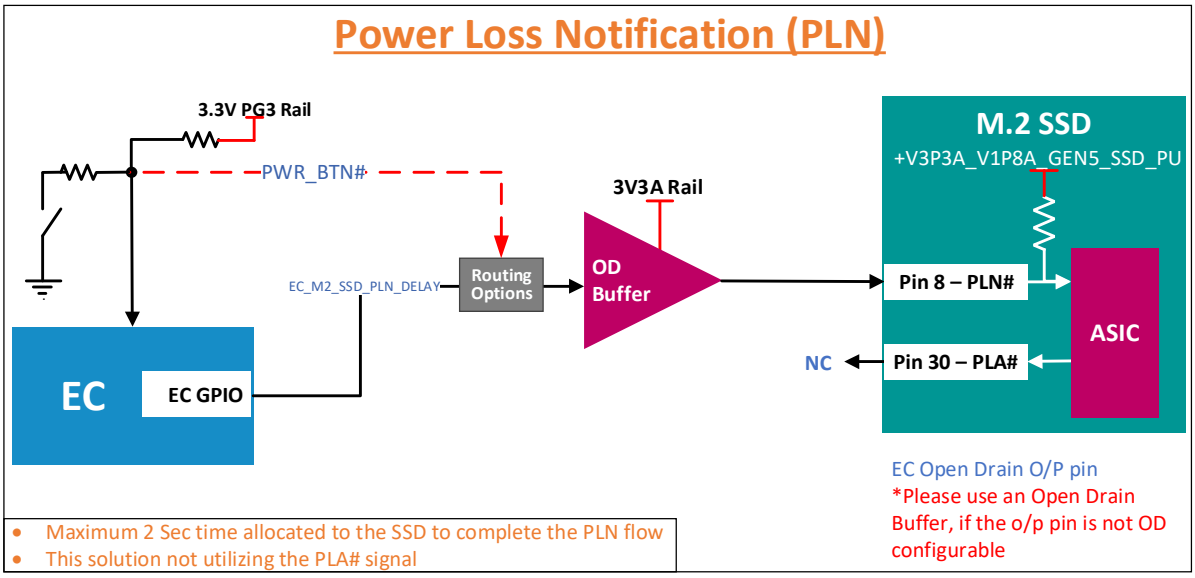


Figure 10-3: Power Loss Notification circuit implementation

10.7.3. BIOS recovery architecture

NVMe BIOS recovery feature supports on SSD which is connected to PCIe Gen5 lane on SOC.

10.7.4. SPI Descriptor Recovery

SPI Descriptor recovery in NVL is achieved by Descriptor verification (Detection) and recovery by the SPI controller in SOC. Since the Descriptor is required for any firmware to be loaded, it can't be recovered by firmware component.

SPI Descriptor are used in SPI FLASH to access control of the SPI FLASH regions to different masters & specify various properties of these regions. If a SPI-Descriptor gets corrupted the platform will not be bootable. To recover from SPI-Description corruption, the SPI flash will now contain 3 descriptors & the SPI controller in SOC is modified to read the subsequent descriptor if it finds a corrupted descriptor. This will enable the system to boot even in the presence of 2 corrupted descriptor.

There are 2 straps used for SPI Descriptor recovery, mentioned below:

Table 41: SPI Descriptor Recovery Strap details

GPIO Pin	Strap Details	Strap Functionality	Comment
xxgpp_h_1	SPI FLASH Descriptor Recovery strap	0= Recovery Disable (Default) 1= Recovery Enable.	Weak Internal 20K PD, Sampled at RSMRSTB.
xxgpp_h_2	SPI Flash Descriptor recovery source selection strap	0=Flash descriptor recovery internal source (Default) 1= Flash descriptor recovery external source	Weak Internal 20K PD, Sampled at RSMRSTB.

10.7.5. NVMe Recovery

If the BIOS/CSME partition in the Flash is corrupted, this feature enables the EC to use an out of band mechanism (I2C/SMBUS) with the NVMe drive & rewrite the BIOS/CSME partition into SPI flash. This enables the system to boot in the presence of a corrupted BIOS partition in SPI-NOR. To support this feature, the following are implemented in the design,

- The firmware issue detection & recovery occur in pre-boot stage. Hence, EC and primary M.2 SSD shall be powered up and running before CPU/PCH is enabled.
- When NOT using the recovery mode, the SSD shall be power gated (off) in Sx.
- EC can override the SSD power while in Sx for the recovery.
- EC shall access M.2 SSD secondary partition over I2C/SMBus signals during recovery mode. Level translator is used to convert EC driven 3.3V I2C/SMBus signals to M.2 SSD 1.8V levels.
- EC shall have recovery indication signal (GPIO).
- Flash descriptor override strap is sampled at RSMRST in NVL silicon to enable CSME recovery in MAF mode. EC firmware needs to wait for 100ms before trying to access the SPI flash after FDO strap is sampled high to prevent any conflicting case where SoC & EC both are trying to access SPI flash.
- EC Recovery indication GPIO should drive Flash descriptor override strap (Active high) of SOC as high to hold CSME communication with Flash Chip.

Note: **NVMe recovery in** MAF mode is not POR for RVP

- In MAF mode during BIOS/CSME recovery, platform power sequencing will be halted at SLP_S3. This is because in MAF mode, for EC to access the SPI flash the eSPI & SPI interface needs to be alive & for that we need RSMRST to be high. So, we can't halt at RSMRST, so we halt at SLP_S3 signal.
- In G3/SAF mode during BIOS/CSME recovery, platform power sequencing will be halted at RSMRST. This is because in G3/SAF mode, EC can directly access the flash so we can halt at RSMRST also.

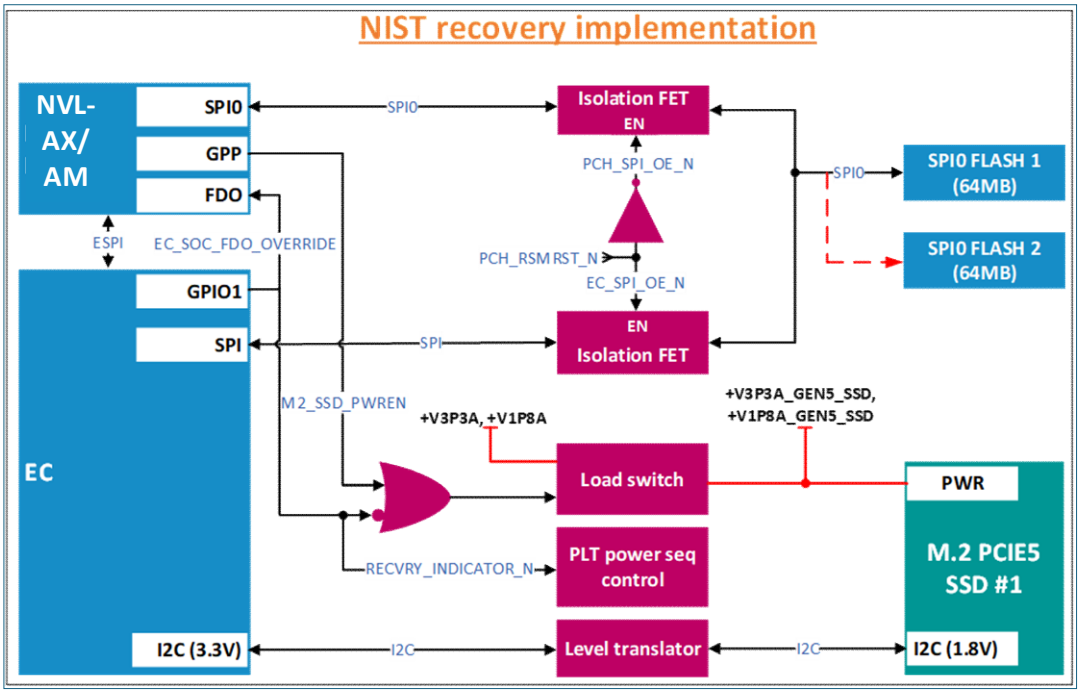


Figure 10-4: NIST193 Recovery Hardware implementation block diagram

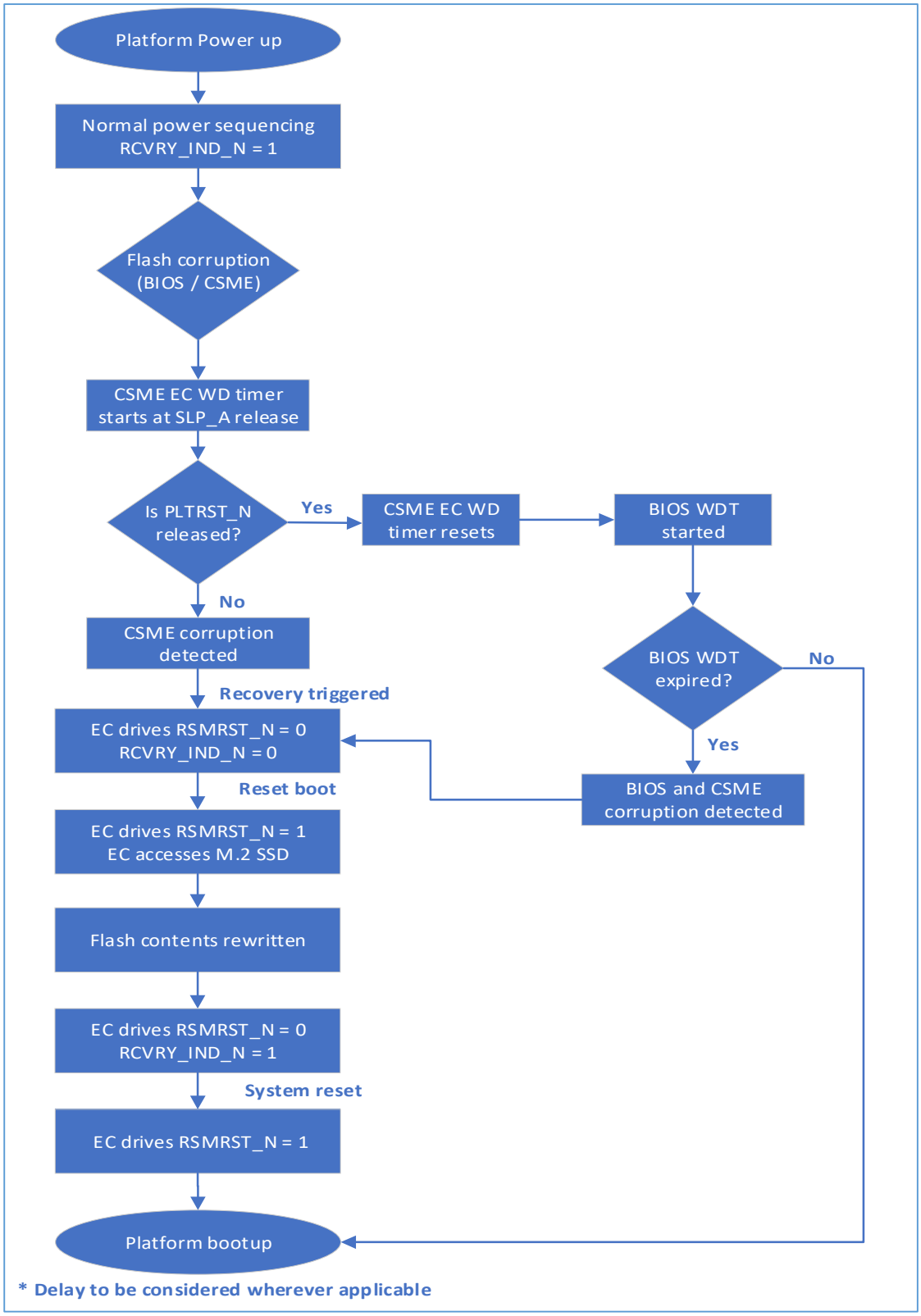


Figure 10-5: MAF Recommended Platform Flow

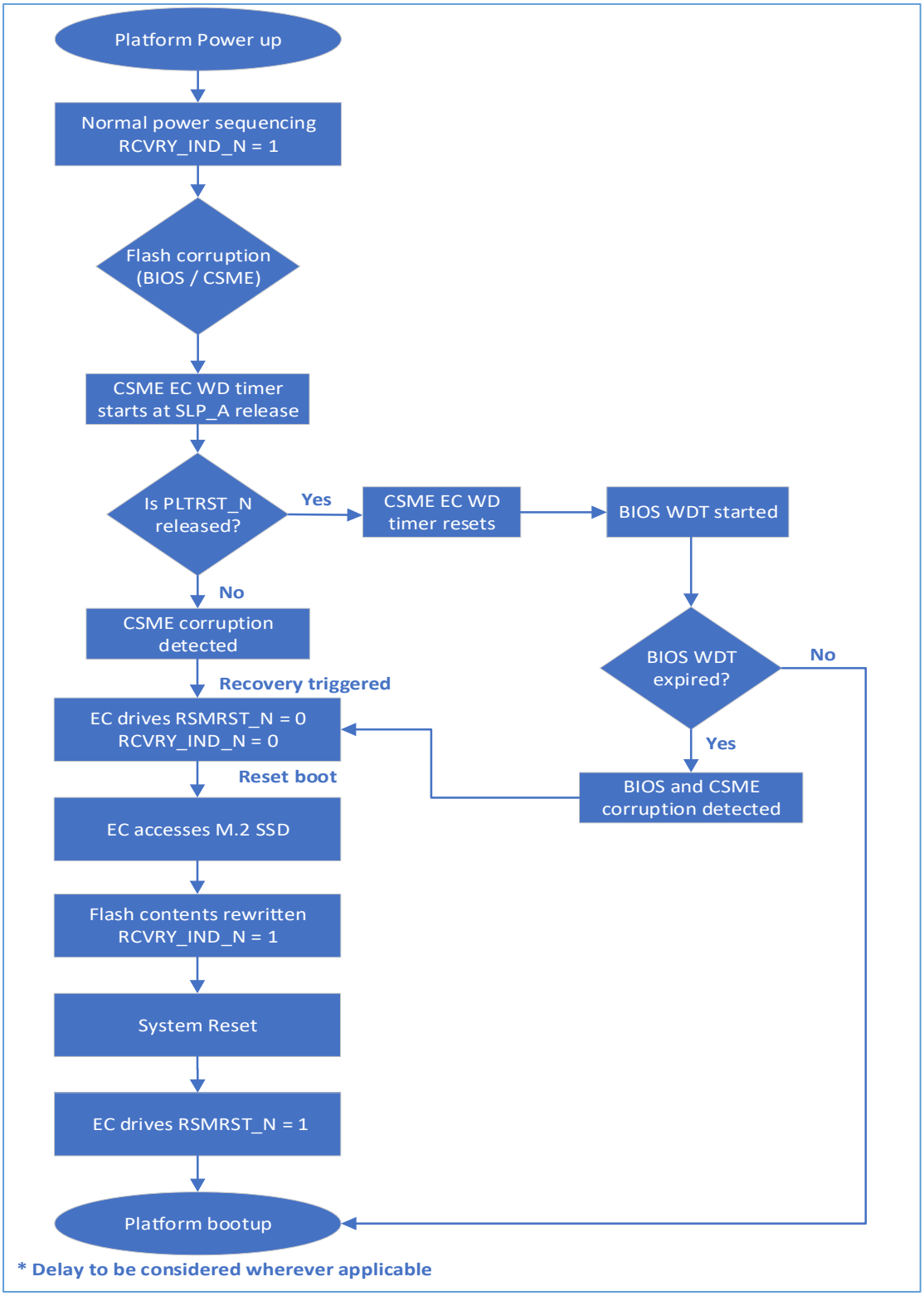


Figure 10-6: SAF/G3 Mode recommended Platform Flow

10.8. UFS

UFS is Not POR for NVL-AX

10.8.1. SD card over PCIe DT CEM Slot

On the NVL-AX the PCIe to SD card interface is validated using the SD Express AIC based on Realtek RTS5264 and will be plugged on to x2 PCIe Slot (on x4 Connector).

10.9. Test plan link (RVP/ SIV)

Will be updated for HAS1.0 release.

11. Connectivity

11.1. Overview

The primary connectivity interface for the NVL AX/AMRVP lies with the SoC. Main connectivity options are Gbe LAN and WiFi. The NVL AX/AM SoC supports integrated connectivity CNVi core (step PHY) which eliminates the need for an external WiFi chip.

WWAN is not a POR for NVL. Connection options for WWAN are not provided in NVL AX/AM RVP

Note: There is no RTD3 load Switch support for WLAN in NVL RVP and the corresponding load switches for enabling power is no longer supported in NVL RVP like PTL UH RVP.

11.2. Connectivity domain platform MRD/PRD

Below is the platform MRD/ PRD for the Connectivity domain.

- Platform MRD HSD link.
- Connectivity Domain platform PRD HSD link

11.3. Connectivity domain RVP LZ/ PRD

TBD

Refer the table below for NVL RVP Landing Zone for Connectivity.

Table 42: RVP LZ for Connectivity solutions in NVL AX/AM RVPs

Si#	Feature	RVP AX/AM
1	**WLAN: M.2 Key-E support for both integrated & Discrete module**	Yes, M.2 Key E module
2	**BT: M.2 Key-E support for both integrated & Discrete module**	Yes, M.2 Key E module
3	**WWAN: M.2 Key-B**	Not POR
4	**WWAN: GNSS (only Integrated GPS Support)**	Not POR
5	**Integrated Gbe Lan – Jacksonville**	Yes
6	**Discrete Gbe LAN - Foxville AIC**	Yes, Via x1 PCIe Gen4 CEM slot (on x4 Connector)

11.4. HW BOM/ Module Details

The table below gives the list of modules supported on NVL AX/AM RVP SKUs as connectivity solutions.

Table 43: POR modules supported for Connectivity Solution

Si#	HW BOM Description	Part#/ IPN	Vendor
1	**Integrated CNVIo**	Whale Peak 2	Intel
2	**Integrated CNVIo**	Spider Peak 2	Intel
3	**Integrated CNVIo**	[1]Pelican Peak	Intel
4	**Discrete WLAN+BT**	Typhoon Peak	Intel
5	**Discrete WLAN+BT**	[2]Breeze Peak	Intel
6	**Gbe LAN**	Jacksonville (device down)	Intel
7	**Gbe LAN**	Fox-Ville Add-In Card	Intel

1: Post TTM WiFi8 support

2: Supported but not POR.

11.5. Connectivity High level block diagram

The figure below shows the high-level block diagram for the connectivity solutions in NVL AX/AM RVP.

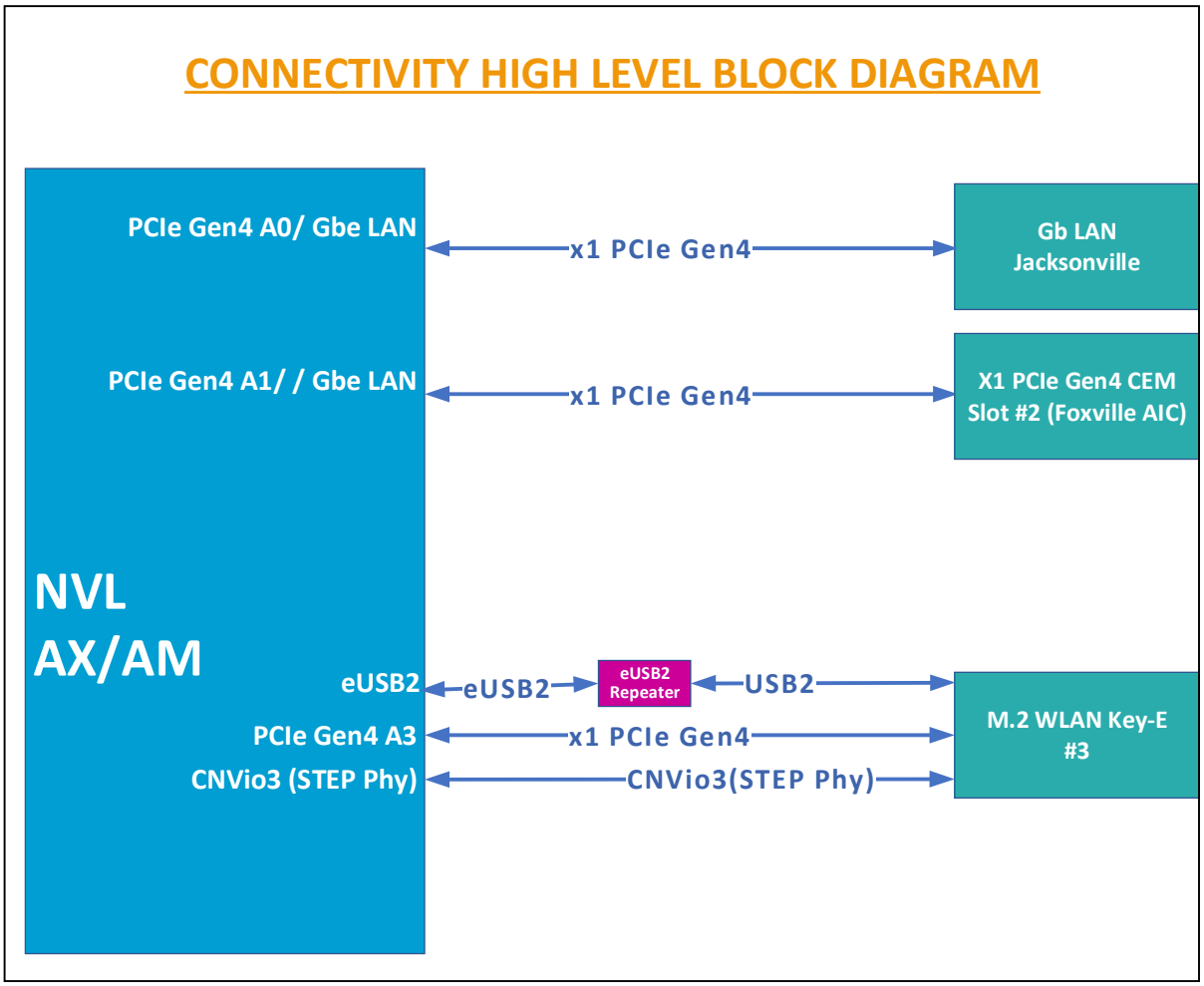


Figure 11-1: NVL AX/AM Connectivity High level Block Diagram

11.6. Connectivity Integration (CNVi)

The RVP supports a M.2 Hybrid Key E slot for Wireless connectivity solutions, it supports a Combo WiFi + BT M.2 module. The Wi-Fi interfaces are over integrated CNVio3(STEP) or x1 PCIe port while the Bluetooth connectivity is supported over CNVi, USB2 or UART+I2S interfaces based on modules is getting plugged in.

Connectivity integration (CNVi) is a general term referring to a family of connectivity solutions which are based on the hard macro (Scorpious) embedded within Intel Silicon. Besides the Scorpius, the CNVi contains an external RF companion module (CRF) and RF antennas. This module will be implemented as a M.2 (2230) module solution on NVL RVP. For Integrated WiFi and Bluetooth, STEP I/F/ TX/RX and RGI/BRI signals are used respectively. For discrete WiFi x1 PCIe is used and for discrete Bluetooth-USB2.0 and UART signals are used. In the diagram below, all necessary signals from NVL AX/AM to the M.2 Key E connector has been shown.

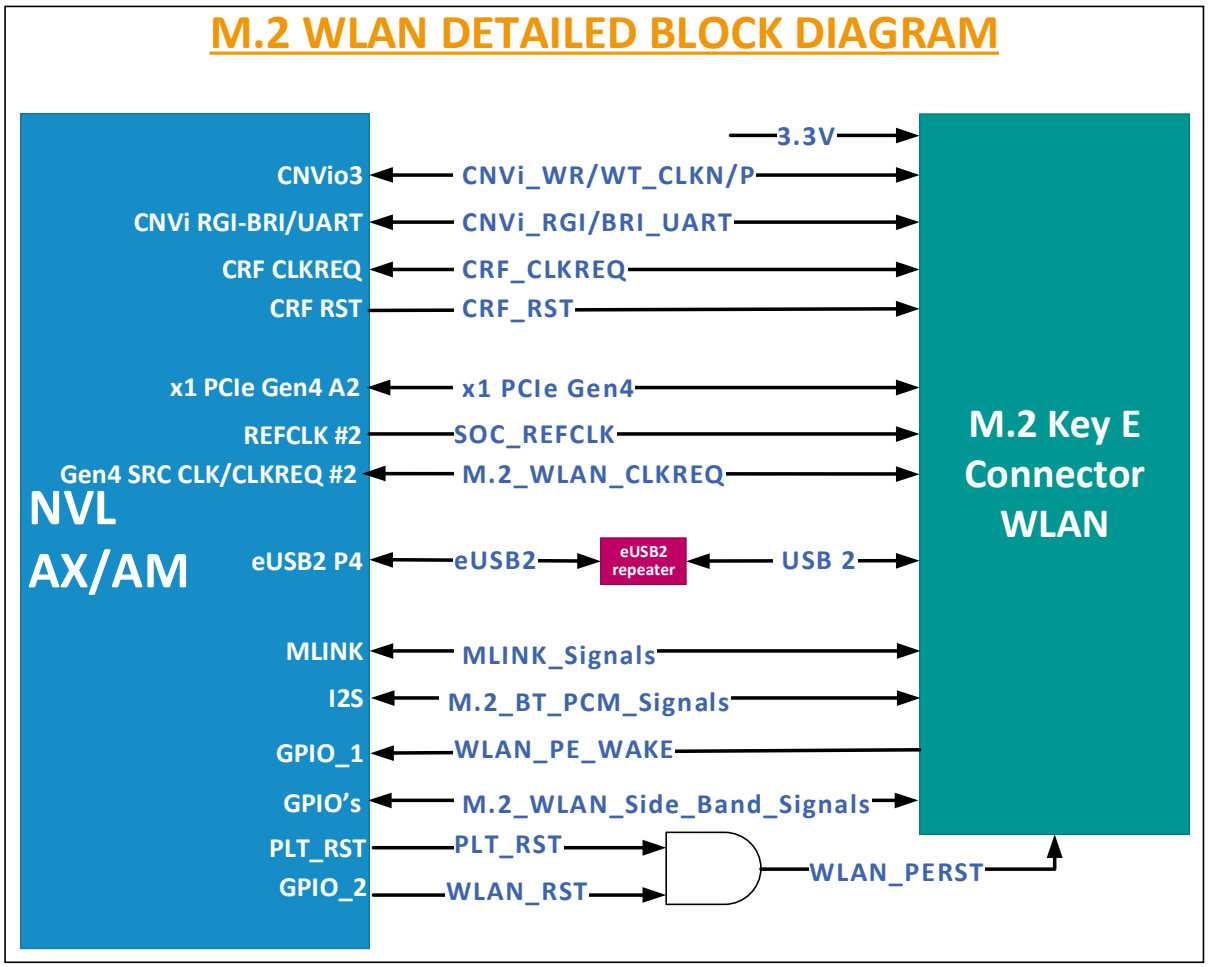


Figure 11-2: NVL AX/AM RVPs M.2 Key E WLAN detailed block diagram

11.6.1. M.2-1A Key E Connector

Next generation WLAN modules need more power to meet performance and feature targets. M2 specification is restricting these features due to the limited current supply (2.5A) allowed in the connector specification.

The new M.2-1A connector will support 1A per pin, with 4pin it will support 4A. New mechanical key allowing current M.2 and New M.2-1A insertion but not allow M.2-1A to work in old M.2 connectors.

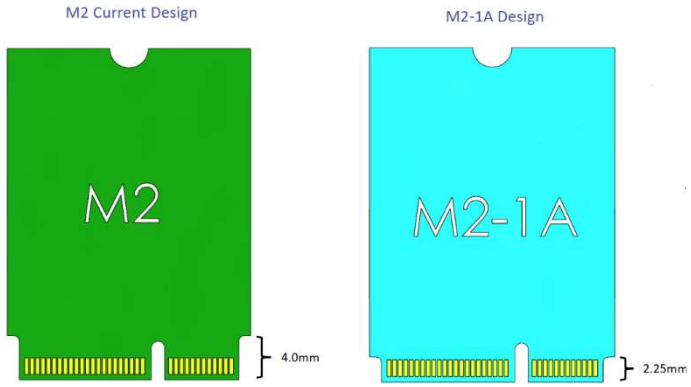


Figure 11-3: New M.2-1A design

11.7. WWAN M.2 Module

Not POR for NVL-AX/AM

11.8. GbE LAN

NVL-AX/AM RVP supports Wired Gigabit Ethernet interface through on-board Intel 1000Base-T PHY LAN Controller I219 (Jacksonville) that connects to PCD through an x1 PCIe interface. LAN PHY operates in Gen1 PCIe mode.

2.5G Base-T MAC/PHY LAN Controller I225 (Foxville) based wired Ethernet will be validated through AIC. SMLink would be provided for Foxville AIC. The LED indications for connectivity status of GbE LAN are listed in table below.

Table 44: LED Definition for RJ45 Connector

Si#	LED Function	State Description
1	Speed	OFF: 10Mbps GREEN: 100Mbps YELLOW: 1Gbps
2	Activity	GREEN: Link is up there no activity on the lines GREEN BLINKING: Tx / Rx or both Activity on the lines

11.8.1. Jackson Ville Controller

The Ethernet Connect I219 is a single-port Gigabit Ethernet Physical Layer Transceiver. It connects to an integrated Media Access Controller (MAC) through a dedicated interconnect. I219 supports operation at 10/100/1000 Mb/s data rates. The figure below shows the detailed block diagram for Jacksonville.

Refer the Intel® Ethernet Connection I219 Datasheet here : RDC link

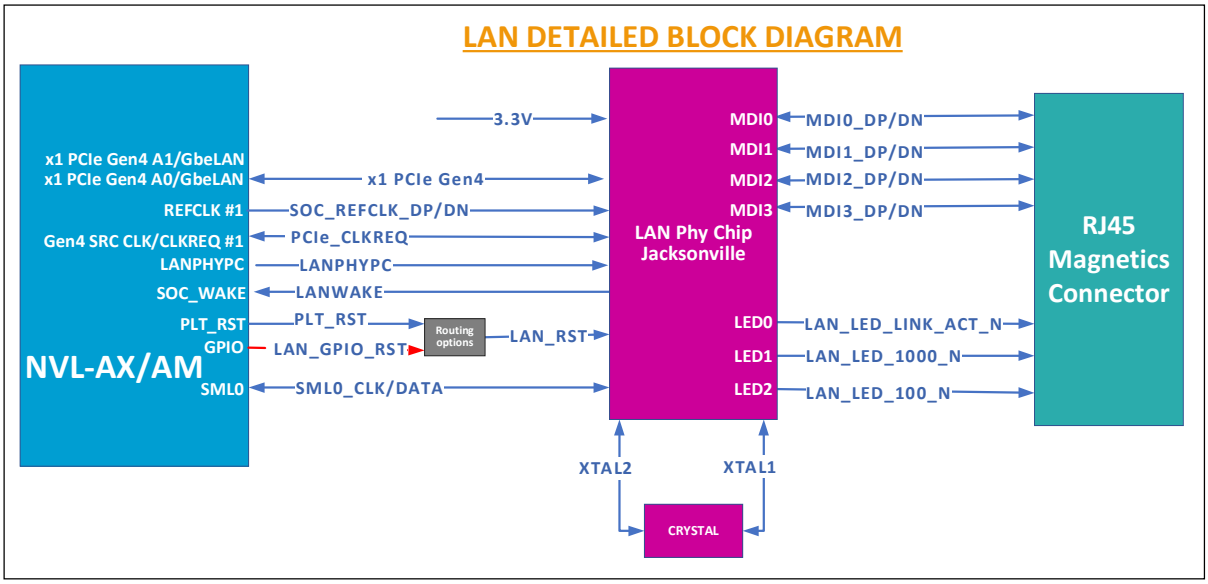


Figure 11-4: NVL AX/AM Jacksonville (On board) level Block Diagram

11.8.2. Foxville Controller

The Intel® Ethernet Controller I225 (I225) is a single-port, compact, low power Gigabit Ethernet (GbE) controller. It is a fully integrated GbE Media Access Control (MAC) and Physical Layer (PHY) device, offering 10/100/1000/2500 Mb/s data rates. The interface-to-host system is a one lane PCI Express* (PCIe*) Gen 2 version 2.1.I225 supports the following features:

- 802.1q VLAN support
- Support for AMT / Intel® vPro™ Technology
    - Host onboard & Dock
    - Intel Stable Image Platform Program (SIPP™) support

On the NVL RVP the Foxville controller is validated by using the Foxville AIC plugged on to x1 PCIe DT Slot (x4 Connector)

11.9. Test plan link (RVP/ SIV)

Will be updated for HAS1.0 release.

12. USB 3.2, USB2.0 & eUSB2

12.1. Overview

NVL AX/AM PCD die supports 8 eUSB2 ports and NVL PCH IOE supports 14 USB2.0 Ports.

eUSB2 is introduced newly in NVL. As the silicon processes continue to advance, there is a growing challenge to support high voltage IO integrations, such as 3.3V based USB 2.0 PHY. The eUSB2 technology is developed to offload the USB 2.0 PHY and serves as a repeater to bridge between and eUSB2 PHY that is 1.2V based and the 3.3V USB 2.0 PHY off the SoC.

Specification for eUSB2:

- eUSB2 Repeater Platform Component Specification (PCS):https://cdrdv2.intel.com/v1/dl/getContent/791949
- eUSB2 + PD integrated spec: https://cdrdv2.intel.com/v1/dl/getContent/793958

12.2. NVL AX/AM USB MRD/ PRDs

Below are the platform MRD/ PRD for the eUSB2/ USB2 domain.

- Platform MRD HSD link.
- PRD for USB domain PRD HSD link.

12.3. USB Features Supported (RVP LZ/ PRD)

12.3.1. RVP PRD for USB

TBD

12.3.2. NVL AX/AM USB 3.2 *Port Mapping*

Below table captures USB 3.2 Port mapping on NVL AX/AM RVP.

Table 45: NVL AX/AM USB 3.2 Port mapping

Domain Feature	Type A Port #	Implementation
USB3.1/2 Type-A Ports (not from TCSS ports) from SoC	**Port 1**	**Default Option:** 1x No's - USB3.2 Gen2 **with redriver** Type-A Port
	Port 2	**Default Option:** 1x No's - USB3.2 Gen2 **with redriver** Type-A Port
USB3.1/2 Type-A Ports from PCH IOE	Please find mapping in Block Diagram	4x No's - USB3.2 Gen2 w/ redriver Type-A Ports

12.3.3. NVL AX/AM eUSB/USB 2.0 Port Mapping

Below table captures eUSB port mapping on NVL AX/AM RVP.

Table 46: NVL AX/AM PCD LZ - eUSB2 Port mapping

eUSB2 Port #	RVP 01	
	Default	Rework #

eUSB2 #1	Type-C Port #0	2x5 USB PPV HDR #1
eUSB2 #2	Type-C Port #1	
eUSB2 #3	Type-C Port #2	
eUSB2 #4	M.2 WLAN	#2. Type-C Port #0
eUSB2 #5	USB3.2 Gen2 w/ redriver Type-A WP #1	
eUSB2 #6	USB3.2 Gen2 w/ redriver Type-A WP #1	
eUSB2 #7	CRD CPHY-DHY Connector 1	#1. CRD CPHY-DHY Connector 1 #2. 2x5 USB PPV HDR #2
eUSB2 #8	USB2 FPS	#1. eUSB2 FPS #2. 2x5 USB PPV HDR #2

Below table captures USB 2.0 port mapping on NVL AX/AM RVP.

Table 47: NVL AX/AM PCH LZ - USB2 Port mapping

USB Port#	RVP 01
USB2 #1	USB3.2 Gen2 w/ redriver Type-A Port #3'
USB2 #2	USB3.2 Gen2 w/ redriver Type-A Port #4'
USB2 #3	USB3.2 Gen2 w/ redriver Type-A Port #5'
USB2 #4	USB3.2 Gen2 w/ redriver Type-A Port #6'
USB2 #5	Rework: FPS
USB2 #6	NC
USB2 #7	NC
USB2 #8	NC
USB2 #9	NC
USB2 #10	NC

USB2 #11	NC
USB2 #12	NC
USB2 #13	NC
USB2 #14	NC

12.4. NVL AX/AM RVP USB3.2 Block Diagram

Below block diagrams captures the USB3.2 mapping on NVL AX/AM RVPs.

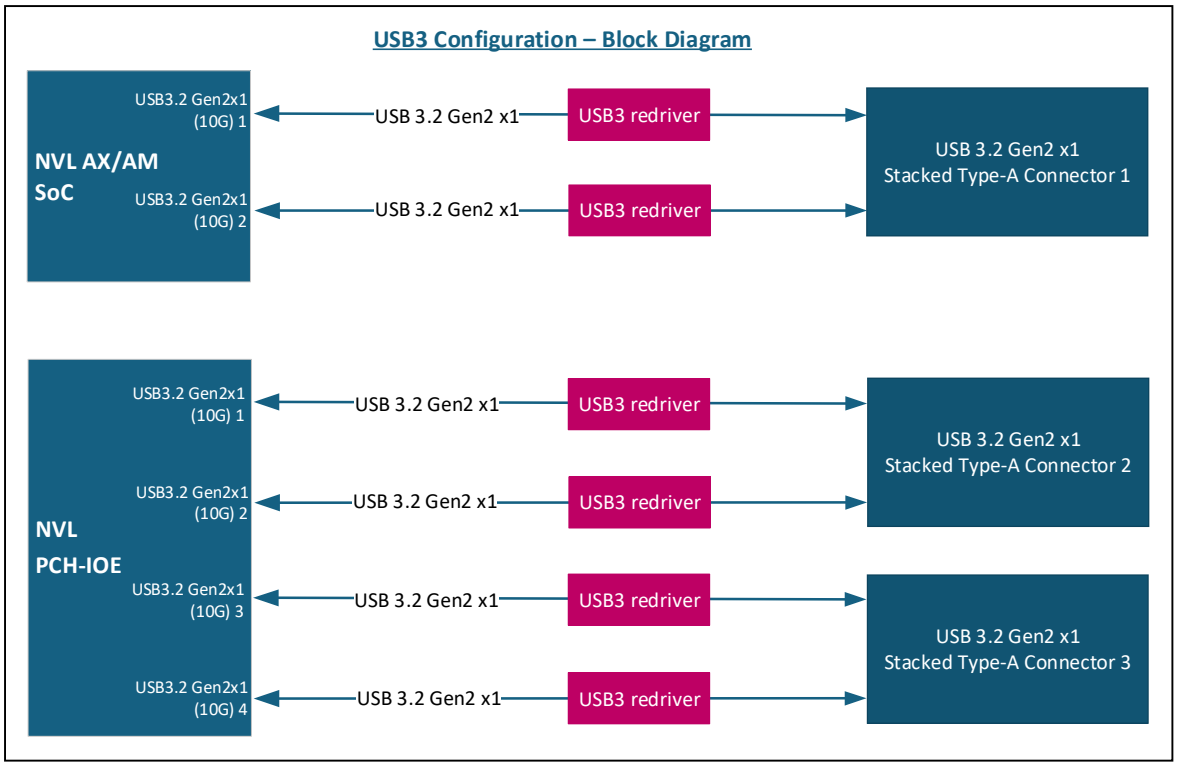


Figure 12-1: USB3.2 High Level Block Diagram

12.5. NVL AX/AM RVP: eUSB2 and USB2.0 Mapping

Below image captures eUSB2 and USB2.0 Mapping on NVL AX/AM RVP.

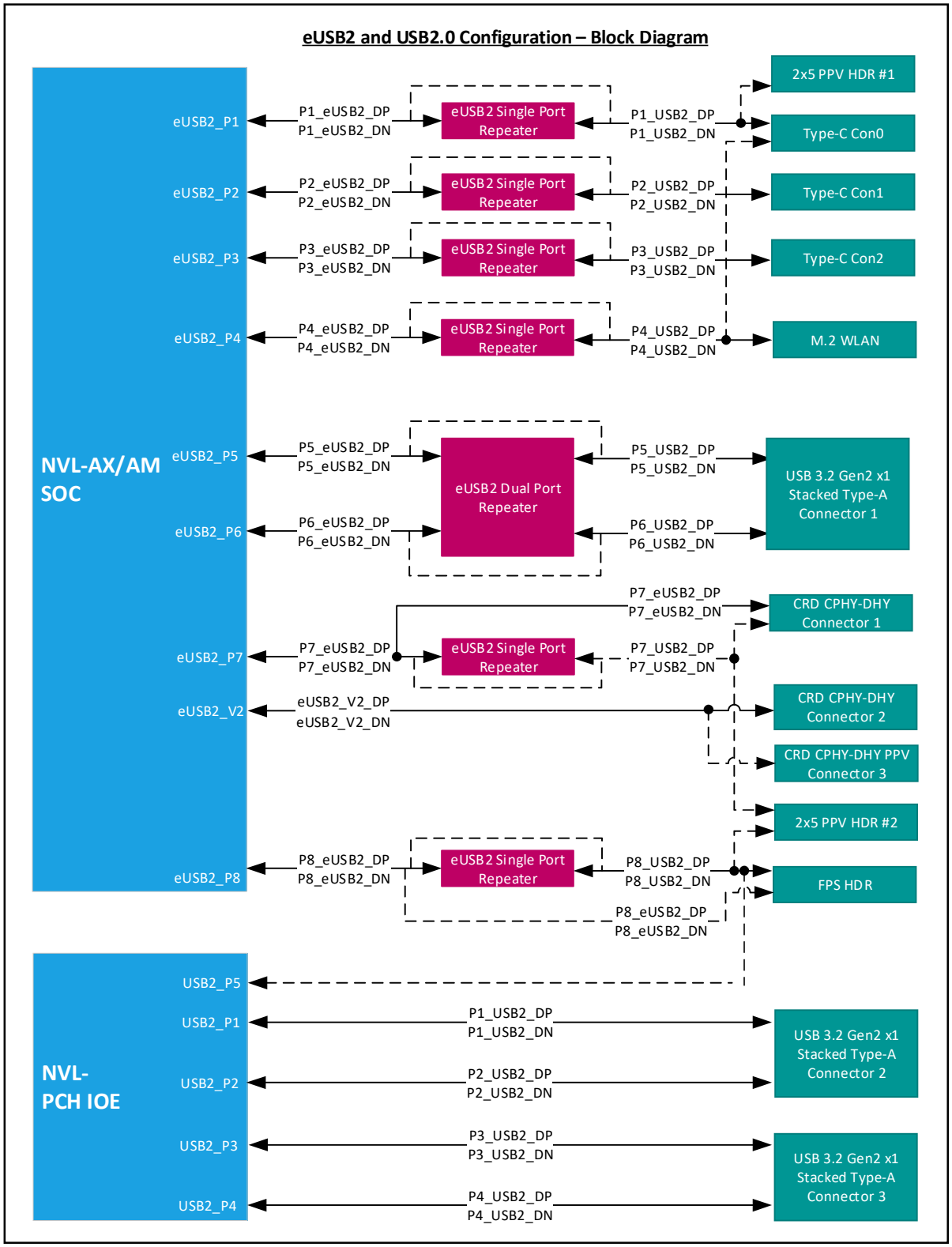


Figure 12-2: PCD eUSB2 and PCH USB2 High level block diagram

NVL AX/AM PCD die has implemented programmable USB OC signals. 4 OC pins are to be shared across the Type-C, USB2.0 & USB3.2 Gen2x1 Type-A ports. This allows the platform designer flexibility in routing of the OC pins & allows for unused pins to be configured as GPIOs. The current limits for the USB3.2 Gen2x1 Type-A ports is set to 1.5A typical.

Table 48: OC Protection from the individual OC protection controllers in NVL AX/AM PCD RVP

Pin Name	NVL AX/AM PCD Configuration
Virtual	Type C port – TCP0 Type C port – TCP1 Type C port – TCP2
GPP_E9_USB2_OC0_N	USB3.2 Connector 1 USB3.2 Connector 2
GPP_B15_USB2_OC3	TCSS Module - Type-A over TCP module

We have 8 OCB Signals from NVL-PCH. These signals can be used to detect overcurrent indication of USB2 Signals from PCH.

Table 49: OC Protection from the individual OC protection controllers in NVL PCH-IOE

Pin Name	NVL PCH-IOE Configuration
GPP_H5_USB2_OCB_0	USB3.2 Stacked Connector 1
	USB3.2 Stacked Connector 2

12.6. HW BOM

12.6.1. NVL AX/AM eUSB/USB2.0 HW BOM

Below are the hardware BOM items used in eUSB/ USB2.0 validation on NVL AX/AM RVP.

Table 50: NVL AX/AM eUSB/ USB2.0 HW BOM

Si#	HW BOM Description	Part#/ IPN	Vendor
1	**eUSB2 repeater - single port**	TI: TUSBE111BC1(WCSP/QFN) **NXP: PTN3222GM (QFN), PTL3222DUK (WLCSP12 with auto resume)** Diodes: PI3EUSB1181 (QFN) RTK: RTS5430S-GR (QFN) Analogix: ANX7461 (QFN) In NVL AX/AM we will go with **NXP Part** (N23582-001) as single port eUSB2 repeater.	TI/ NXP/ Diodes/ Realtek/ Analogix
2	**eUSB2 repeater - dual port**	TI: PTUSB2E2211001VBWR Diodes: PI3EUSB1182 Realtek: RTS5430D-GR (QFN) In NVL AX/AM we will go with **TI Part** (N71710-001) TUSB2E2211 Part as dual port eUSB2 repeater.	TI/ Realtek/ Diodes

12.6.2. NVL AX/AM USB 3.2 HW BOM

Below are the hardware BOM items used in USB 3.2 validation on NVL AX/AM RVP.

Table 51: RVP HW BOM for USB3.2

Si#	HW BOM Description	Part#/ IPN	Vendor
1	USB3.2 Redriver Part	MPN: PI3EQX1002E2ZREX IPN: J41453-002	Diodes

12.7. USB Signal Protection

NVL AX/AM RVP shall have a CMC and ESD diodes for Signal protection as suggested by PDG.

12.8. USB Debug Support

DNX and Early Platform Debug via the USB subsystem requires both the Host and Device controllers and associated PHYs to be operational prior to the Host Group/Sub System. This also implies that all other USB subsystem ingredients also be operational along with the controllers. This change to enable the USB subsystem at a much earlier phase is required to enable two key features:

- Early Enabling of USB based platform debug also known as DCI.DBC or EXI-over-BSSB
- Download And Execute (DNX)-Zbbed

For more details on USB debug please refer to Chapter 07 - USB Debug

Table 52: USB Debug Support on NVL AX/AM RVP

Connector Details	Supported Topologies
Connector1: Type-A USB Walk-Up Port USB3.2 Gen 2x1_Port 1 & eUSB2_Port5	USB2.DbC USB3.DbC
Connector2: Type-A USB Walk-Up Port USB3.2 Gen 2x1_Port 2 & eUSB2_Port6	USB2.DbC USB3.DbC
Type C Port 0: eUSB2_Port1	USB2.DbC (Early DbC) USB3.DbC
Type C Port 1: eUSB2_Port2	USB2.DbC USB3.DbC
Type C Port 2: eUSB2_Port3	USB2.DbC USB3.DbC

12.9. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

13. Audio

13.1. Overview

NVL AX/AM RVP enables value system with single-chip audio solution. On board codec is the ALC722-CG [SDCA 0.8] compliant Soundwire based codec which can be configured in SNDW3 multilane or SNDW1 single lane mode. Refer ALC722 CODEC section for more detail.

RVP supports different audio codecs validation through add-in-card solution. Realtek AIOC GEN6 is the POR AIC for NVL & Cirrus AIC v3 will support delta validation configuration and existing Realtek AIOC GEN3 to support HDA [ALC245] validation. Refer AUDIO AIC section for more detail.

13.2. Audio domain platform MRD/PRD

Below is the platform MRD/ PRD for the Audio domain.

- Platform MRD HSD link.
- Audio Domain platform PRD HSD link.

13.3. Audio domain RVP LZ/ PRD

TBD

The below is the RVP LZ for audio interface. We have ALC722 audio codec soldered down in RVP.

Table 53: Audio Domain RVP feature support

Sl No	Domain Feature	Silicon Port	AX/AM RVP
1	**Audio jack codec (SNDW based) MB solder Down**	SNDW3 **(default)/** SNDW1 **(rework)**	Yes
2	**Audio HDR - JA (HDA/I2S based Codec)**	HDA **(default)/** I2S0 **(rework)**	Yes
3	**Audio HDR - JD (DMIC/ Amplifier)**	SNDW 1/ DMIC 1 SNDW 2/ DMIC 0	Yes
4	**Audio HDR - JE (SNDW multilane codec)**	SNDW 0 **(default /** SNDW 3 **(rework)/** I2S 1 **(rework)**	Yes
5	**M.2 Key-BT**	I2S2 **(rework)**	Yes

13.4. Audio domain HW BOM

Below table captures the HW BOM for Audio.

Table 54: Audio Domain HW BOM

SL #	BOM Description	Part number	Vendor	HSD Link
1	**Sound wire - All in one codec (DMIC, SPKR, UJACK) MB solder down**	ALC722-CG (SDCA)	Realtek	TBD
2	**Sound wire - HDA codec (Gen4 card) - Desktop solder down/ Mobile is AIC**	ALC256	Realtek	TBD
3	**Sound wire - All in one codec (DMIC, SPKR, UJACK)**	1. ALC712-VB (SDCA)	1. Realtek	TBD
	Audio Gen6 AIOC or updated Gen	2. CS42L43 (Cohen)	2. Cirrus	
4	**Sound wire - Jack codec**	1. ALC713-VB (SDCA)	1. Realtek	TBD
5	**Sound wire - Stereo amp**	1. ALC1320 (SDCA)	1. Realtek	TBD
		2. CS35L56 (Jamerson)	2. Cirrus	

13.5. AIC List

Below is the AIC list for audio supported on NVL RVPs.

Table 55: AIC list for audio supported on NVL RVPs

Si#	Add In Card (AIC) Description	IPN	Rev #	Wiki link
1	**Realtek AIOC Gen6 (Golden Config)**	3PE	-	https://wiki.ith.intel.com/display/ITSDesignWiki/Gen+6+Audio+Add-In-Card
2	**Cirrus AIOC v3 (3* Delta Config)**	3PE	-	https://wiki.ith.intel.com/display/ITSDesignWiki/Cirrus+AIOC+v3
3	**Realtek AIOC Gen4 (Delta Config)**	3PE	-	https://wiki.ith.intel.com/display/ITSDesignWiki/Gen4+Audio+Add-In-Card
4	**TI AIOC Gen 1 (3* Delta Config)- CCB yet to be received**	3PE	-	TBD

13.6. High level block diagram

Below image shows high level block diagram for audio on NVL.

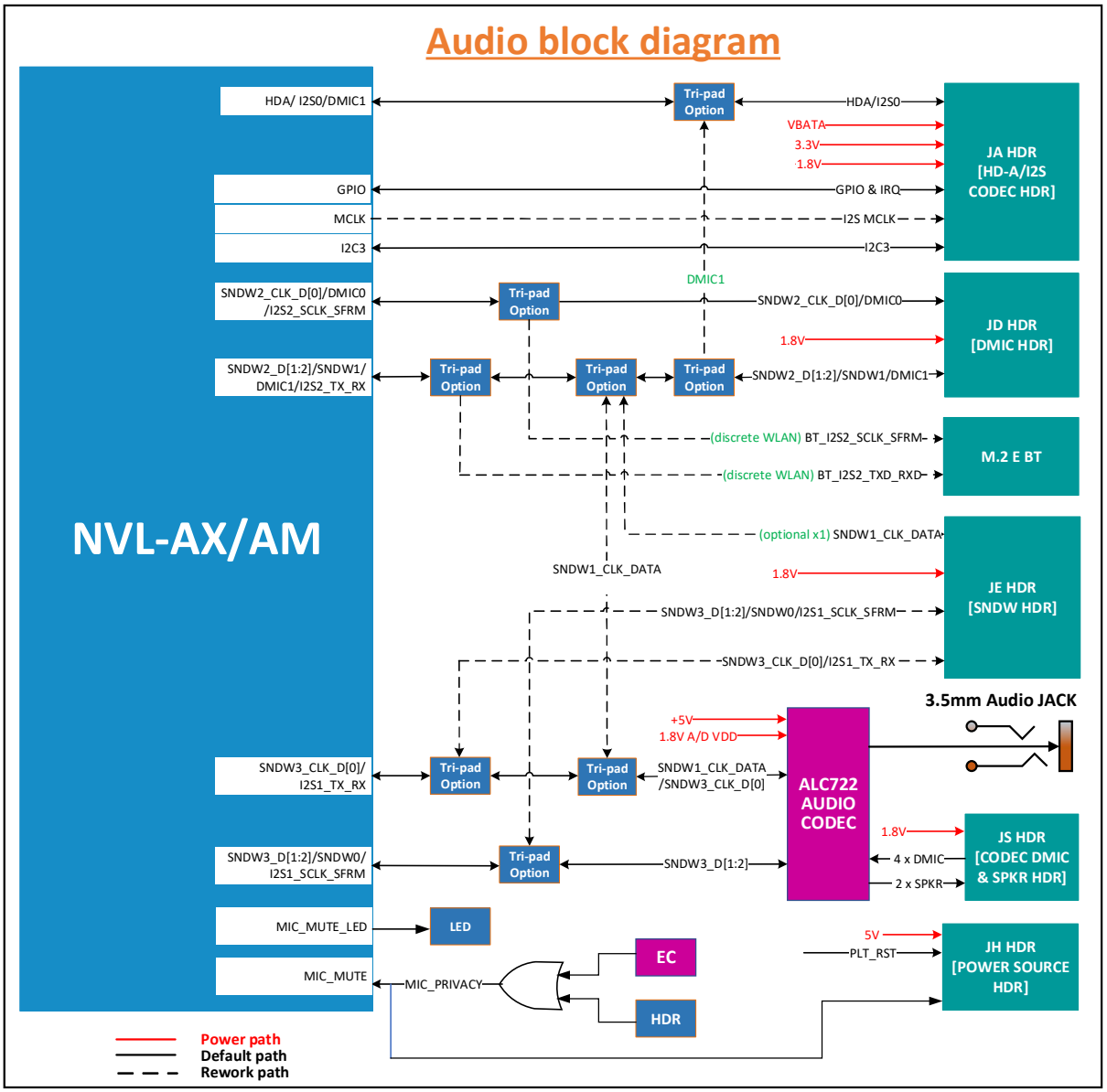


Figure 13-1: NVL RVP Audio high level block diagram(TBD)

13.7. ALC722 SNDW on-board CODEC

- The ALC722-CG is compliant to SDCA v0.8[MIPI04], where SDCA stands for SoundWire Device Class for Audio architecture that standardizes the interface for software to control the audio function through a SoundWire interface.
- The ALC722 integrates a headphone amplifier can drive 15-ohm headphone & supports legacy Universal Audio Jack.
- An integrated stereo Class-D amplifier directly drives the speakers. The Class-D amplifier is designed to drive speakers with as low as 4Ω impedance. The advantage of an integrated Class-D amplifier in the ALC722 is high efficiency with lower power consumption.
- The ALC722 has two stereo digital microphone inputs.
- SNDW3 multilane connects to ALC722 codec by default, SNDW1 single lane can be enabled with a rework option.

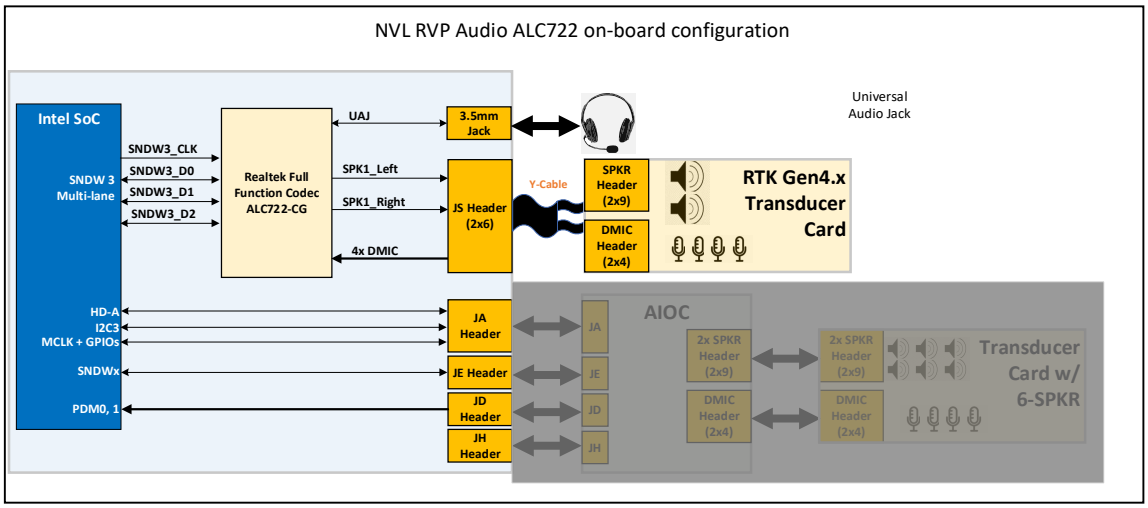


Figure 13-2: NVL RVP Audio ALC722 on-board configuration

13.8. AUDIO AIC Validation Configuration

NVL RVP supports below AIOC (All-in-One Card) with SDCA 1.0 components.

- Realtek AIOC Gen6 (Golden Config)
- Realtek AIOC Gen4 (Delta Config)
- Cirrus AIOC v3 (3* Delta Config)
- TI AIOC Gen 1 (3* Delta Config): CCB Pending

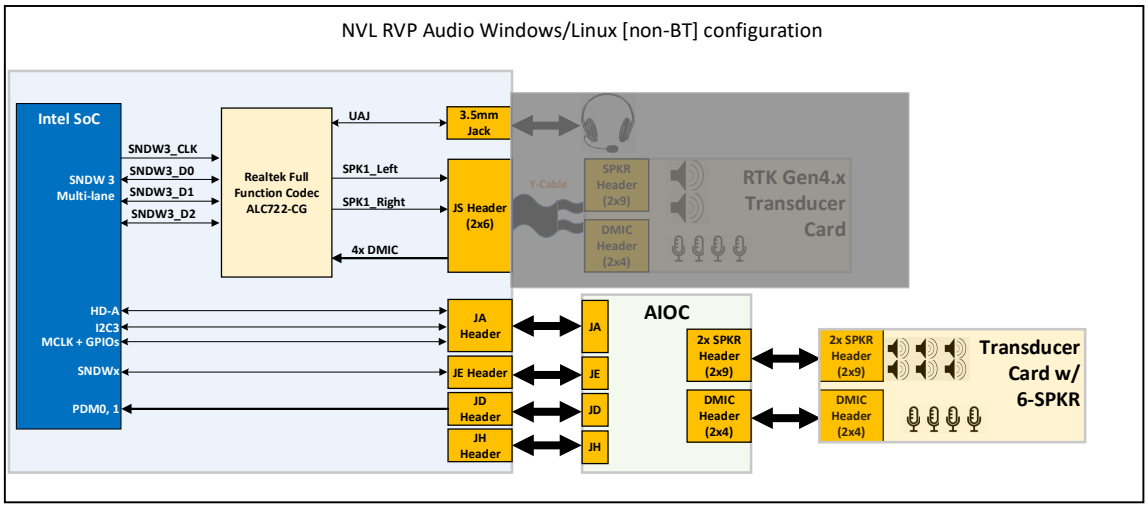


Figure 13-3: NVL RVP Audio Windows/Linux [non-BT] configuration

Note: BT-audio offload support via I2S2 port can be enabled only through resistor rework option on RVP.

Refer below table for AIOC supported CODECs versus validation configuration details.

Table 56: NVL RVP Audio Windows/Linux build validation configuration table (TBD)

Val. Config	AIOC	Driver	Components			I/Os
			Full Function Codec (UAJ, DMIC, Spk Out)	Jack Codec (UAJ, DMIC)	SmartAmp	
GC (5*)	RTK AIOC Gen6	SNDW ACX	1x ALC712-VB	-	1x ALC1320	• 3.5mm UAJ (Hi-Z HP) • 4x speaker (aggregated to stereo) • 4Ch DMIC (ALC712 attached)
4* -1	N/A	SNDW ACX	1x ALC722-CG	-	-	• 1x 3.5mm UAJ • 2x speaker (Class D, simple power limit) • 2/4ch DMIC (ALC722 attached)
4* -3	RTK AIOC Gen6	SNDW ACX	-	1x ALC713-VB	2x ALC1320	• 3.5mm UAJ (Hi-Z HP) • 4x speakers (aggregated to stereo) • 4Ch (ALC713-VB attached)
3*-1	Cirrus AIC v3	SNDW ACX	1x Cohen (CS42L43)	-	6x Jamerson (CS35L56)	• 1x 3.5mm UAJ • 6x speakers (aggregated to stereo) • 2ch DMIC via Cohen
3* -2	TI AIOC Gen1	SNDW ACX	1x TAC5682	-	2x TAS2880 (Stereo)	• 1x 3.5mm UAJ (Hi-Z HP) • 6x speakers (aggregated to stereo) • 4ch DMIC via codec

13.9. RVP Audio Headers

The RVP audio header details can be found in the below Wiki Link

https://wiki.ith.intel.com/display/ITSDesignWiki/Gen+6+Audio+Add-In-Card

NVL silicon supports only 15 audio functionality pins. SoC muxing consideration is driven by CCG Platform team (comprising of Audio Domain Architects, as well as Platform EIO stakeholders) to balance between total GPIO pins needed/reserved for Audio while meeting primary requirements for the different segments (Windows, Chrome, IOT, etc). Pin muxing with reduced pin count for the NVL SoC is shown in the below table.

Table 57: NVL Audio pin muxing

SoC Pin Name	Sound wire 3	Sound wire 2	Sound wire 0/1	DMIC	I2S / PCM	HD-A
GPP_D_10_HDA_BCLK_I2S0_SCLK_HDACPU_BCLK	-	-	-	-	I2SSCLK[0]	HDA_BCLK
GPP_D_11_HDA_SYNC_I2S0_SFRM	-	-	-	-	I2SSFRM[0]	HDA_SYNC
GPP_D_12_HDA_SDO_I2S0_TXD_HDACPU_SDO	-	-	-	-	I2STXD[0]	HDA_SDO
GPP_D_13_HDA_SDI_0_I2S0_RXD_HDACPU_SDI	-	-	-	-	I2SRXD[0]	HDA_SDI0
GPP_D_16_HDA_RST_B_DMIC_CLK_A_1	-	-	-	DMIC_CLKA[1]	-	HDA_RST#
GPP_D_17_HDA_SDI_1_DMIC_DATA_1	-	-	-	DMIC_DATA[1]	-	HDA_SDI1
GPP_D_9_I2S_MCLK1_OUT	-	-	-	-	I2SMCLK[0]	-
GPP_S_0_SNDW3_CLK_I2S1_TXD	SNDW_CLK[3]	-	-	-	I2STXD[1]	-
GPP_S_1_SNDW3_DATA0_I2S1_RXD	SNDW_DATA[3][0]	-	-	-	I2SRXD[1]	-
GPP_S_2_SNDW3_DATA1_SNDW0_CLK_DMIC_CLK_A_0_I2S1_SCLK	SNDW_DATA[3][1]	-	SNDW_CLK[0]	DMIC_CLKA[0]	I2SSCLK[1]	-
GPP_S_3_SNDW3_DATA2_SNDW2_DATA1_SNDW0_DATA0_DMIC_DATA_0_I2S1_SFRM	SNDW_DATA[3][2]	SNDW_DATA[2][1]	SNDW_DATA[0]	DMIC_DATA[0]	I2SSFRM[1]	-
GPP_S_4_SNDW2_CLK_DMIC_CLK_A_0_I2S2_SCLK	-	SNDW_CLK[2]	-	DMIC_CLKA[0]	I2SSCLK[2]	-
GPP_S_5_SNDW2_DATA0_DMIC_DATA_0_I2S2_SFRM	-	SNDW_DATA[2][0]	-	DMIC_DATA[0]	I2SSFRM[2]	-
GPP_S_6_SNDW2_DATA1_SNDW1_CLK_DMIC_CLK_A_1_I2S2_TXD	-	SNDW_DATA[2][1]	SNDW_CLK[1]	DMIC_CLKA[1]	I2STXD[2]	-
GPP_S_7_SNDW3_DATA3_SNDW2_DATA2_SNDW1_DATA0_DMIC_DATA_1_I2S2_RXD	SNDW_DATA[3][3]	SNDW_DATA[2][2]	SNDW_DATA[1]	DMIC_DATA[1]	I2SRXD[2]	-

NVL RVP supports different codec validation via AIC connected through JA, JD, JE & JH headers.

13.10. Privacy Microphone Protection Feature

Privacy microphone protection feature is POR in NVL RVP.

The ACE (Audio Context Engine) IP offers a microphone privacy protection scheme through a HW DMA (Dynamic Memory Access) data zeroing mechanism, if parameter (Microphone Privacy Enable) MICPVCE = 1.

The HW will take in a privacy signaling input from the GPIO pin (which typically connects to a mic disable switch), indicating the current user privacy mode setting on the system.

If the mic disable switch is turned on, and the DfMICPVCP.DDZE policy register indicates privacy mode is enabled, the HW will interrupt DSP FW (if link management is offloaded) / host SW (if link management is not offloaded) indicate the mic disable entry (allow DSP FW / host SW to gracefully [the audio capture stream without any audible glitches), and then mask the data from the microphone to zeros after a time-out period programming in DfMICPVCP.DDZWT register. It also turns on a privacy indicator output through the GPIO pin (which typically connects to a privacy LED).

When the mic disable switch is turned off later, the HW will unmask the data from the microphone (immediately) and interrupt DSP FW indicating the mic re-enabling (allow DSP FW / host SW to gracefully unmute), as well as turning off the privacy LED indication through the GPIO pin.

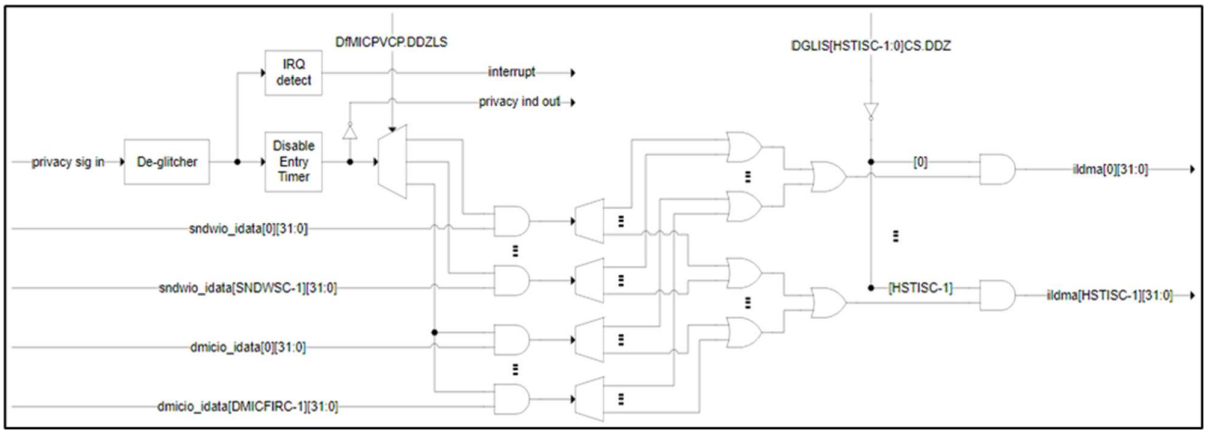


Figure 13-4: Privacy microphone protection conceptual diagram

Reference:

https://docs.intel.com/documents/iparch/ace/ACE%20IP/3.x/Integration%20Specs/PTLSM/PTLSM_ACE3.x_Integration_HAS.html#privacy-microphone-protection

Below table represents the **privacy sig in** & **privacy ind out** signal description.

Table 58: Privacy microphone protection signal description

Signal Names	Type	Description
PVC_SIG_IN	I	**Privacy Signaling Input:** Privacy microphone disable signaling input, typically for connection to a switch. Asserted high to indicate the microphone disabled state (HW will ensure the data output from the microphone is masked to zero).
PVC_IND_OUT	O	**Privacy Indicator Output:** Privacy microphones disable indication output, typically for connection to an LED. Asserted high to indicate the microphone disabled state (after HW has masked the data output from the microphone to zero).

Note: These pins are typically associated with DMIC interface, but also usable by microphone connected over SoundWire interfaces.

NVL RVP uses SoC pins MIC_MUTE and MIC_MUTE_LED to support microphone privacy protection. The below diagram represents RVP implementation.

Table 59: NVL RVP audio MIC privacy support block diagram

Signal Name	Description
GPP_H_16_MIC_MUTE	Mic mute - Indicate the user privacy mode setting on the system (ON: gate the clock to the mic, OFF: ungate the clock to the mic)
GPP_H_17_MIC_MUTE_LED	Mic mute led- Led to Indicate the user privacy mode setting on the system. (ON: gate the clock to the mic, OFF: ungate the clock to the mic)

NVL RVP has **1x3 header** to control the MIC privacy operation. Default header pin [2-3 short] is OFF, when user wants to turn on the MIC mute option then header pin [1-2 short] should be ON. Alternately, MIC mute can also be controlled via EC using scan matric Fn key.

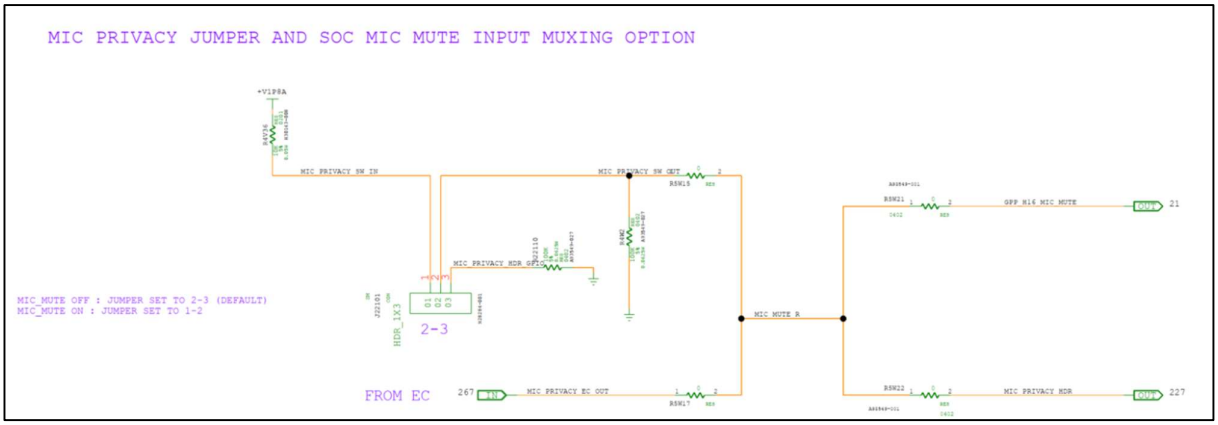


Figure 13-5: NVL RVP audio MIC privacy header

13.11. Audio section circuit optimization

The circuit optimizations done on PTL UH RVP will be carry forwarded to NVL RVP as well.

PTL-UH RVP audio power supply generation optimized with default load switch bypass configuration for all the audio power generation (no RTD3 support) as compared to the load switch controlled in the previous generation of program. RVP team will monitor the no risk in the ERB validation with load switch bypass configuration and completely remove the load switch circuit from AX/AM RVP onwards.

ALC722-CG codec & AIC rails will follow default platform sequencing of **VBATA -> 5V&3.3V -> 1.8V** supply.

Below table captures the audio power rails load current requirement followed in PTL-UH RVP. ALC722 load current requirements are aligned with the Realtek team and AIC power rail requirements are aligned with Realtek/Cirrus.

Table 60: NVL AX/AM audio power requirements (same as PTL)

Source power Domain	Source power rail	Audio section voltage rail	Header/ CODEC	Voltage [V]	Current [mA]	Remarks
+V1P8A	+V1P8DX_ AUDIO_LS	+V1P8DX_AUDIO_ VDD_JA_JE	JA.4, JE.4	1.8V ± 5%	850	
		+V1P8DX_AUDIO_ DMIC_JD_JS	JD.4, JS.4	1.8V ± 5%	300	
		+V1P8DX_AUDIO_ CODEC_ADVDD2	ALC722 AVVD2 supply	1.8V ± 5%	130	
		+V1P8DX_AUDIO_ CODEC_DVDD	ALC722 DVDD supply	1.8V ± 5%	15	
+V3P3A	+V3P3DX_ AUDIO_LS	+V3P3DX_AUDIO_JA	JA.8	3.3V ± 5%	100	
+V5A	+V5DX_AU DIO_LS	+V5DX_AUDIO_ CODEC_PVDD	ALC722 PVDD supply	5V ± 10%	1300	
		+V5DX_AUDIO_ CODEC_AVDD	ALC722 AVDD supply	5V ± 10%	20	
		+V5DX_AUDIO_ DMIC_JH	JH.1	5.0V ± 5%	2300	
		+V5DX_AUDIO_ VDD_JH	JH.2	5.0V ± 5%		
+VBATA	+VBATA_A UDIO_LS	+VBATA_ AUDIO_JA	JA.10	13V ± 5%	1575	19V DC [AC-DC output adaptor] corresponding VBATA = 13V

13.12. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

14. Integrated Sensor Hub (ISH)

14.1. Overview

The Integrated Sensor Hub (ISH) is a Soft IP that serves primarily as the connection point for the sensors on a platform. ISH is designed for the "Always-On, Always-Sensing" goal. NVL supports Integrated Sensor Hub (ISH 5.8). ISH contains the following interface to the sensors namely: I2C, I3C, SPI, UART, GPIO. It provides the following functions to support this goal.

- **ISH I2C:** ISH contains up to 3 I2C Ports capable of High-Speed Mode up to 1 Mbps.
- **ISH I3C:** ISH contains up to 2 I3C Port with HDR/DDR up to 24Mbps.
- **ISH SPI:** ISH contains 1 SPI port supporting speed up to 25 Mbps.
- **ISH UART:** ISH supports 2 UART ports capable of supporting operating speeds up to 4 Mbps.
- **ISH GPIOs**: ISH GPIOs are typically used for enabling the power to the sensor, detecting the interrupts from sensors etc. External pull ups will be provided for ISH GPIOs.

14.2. ISH domain platform MRD/PRD

Below is the platform MRD/ PRD for the ISH domain.

- Platform MRD HSD link.
- ISH Domain platform PRD HSD link.

14.3. ISH domain RVP LZ/ PRD

TBD

Refer the table below for NVL RVP Landing Zone for ISH.

Table 61: RVP LZ for Sensors on NVL RVP

Si #	Feature /Interface	NVL-AX/AM RVP
1	**Sensor AIC**	Yes, via Sensor AIC
2	**Sensors on board**	No
3	**Fingerprint Sensor**	Yes, via FPS HDR (USB2 w/ Eusb2 repeater (Default), Eusb2, GSPI, USB2 from PCH)

14.4. HW BOM

The following sensors are selected for validation on NVL and will be hosted on the MoSAIC Gen 2 card.

Table 62: List of Sensors supported on MoSAIC Gen 2

Si#	HW BOM Description	MoSAIC - BOM1		MoSAIC - BOM2	
		Part#/ IPN	Vendor	Part#/ IPN	Vendor
1	**3-axis Accelerometer**	BMI323	Bosch	ST LSM6DSV256	STMicro
2	**3-axis Magnetometer**	MMC5633NJ	Memsic	AK9919C	AKM
3	**3-axis Gyroscope**	BMI323	Bosch	ST LSM6DSV256	STMicro
4	**2nd Accelerometer**	BMA530	Bosch	ST LIS2DW12	STMicro
5	**Barometer/Altimeter**	-	-	ST LPS22DF	STMicro
6	**HAL switch**	BU52072GWZ	Rohm	BU52072GWZ	Rohm
7	**Short distance proximity sensor (to 30 cm)**	VCNL4030	Vishay	-	-
8	**ALS**	VCNL4030	Vishay	AMS TCS3410	AMS
9	**SAR - Proximity**	SX9331	Semtech	SX9331	Semtech
10	**TOF**	STVL53L8	ST Micro		
11	**Radar for Human Presence**	-	-	BGT60TR13C	Infineon
12	**Miscellaneous**	Samtec cable - HQCD-030-12.00-TBL-SBR-1			
13	**Miscellaneous**	Extender cable - 10-pin 2x5 Socket-Socket 1.27mm IDC (SWD) Cable			

Table 63: List of Other Sensors supported in NVL RVP(TBD)

Si#	HW BOM Description	Part#/ IPN	Vendor
1	AON CVS (Computer Vision Sensing) 3rd party chip	Sabre AIC	Synaptics

14.5. AIC List

MoSAIC Gen2 AIC details are given below.

Table 64: AIC list supported for ISH

Si#	HW BOM Description	Part#/ IPN	Vendor	Wiki link
1	MOSAIC Gen2 AIC	3PE	Intel	MosAIC

14.6. ISH High level block diagram

The figure below shows the high-level block diagram for the ISH on NVL RVPs.

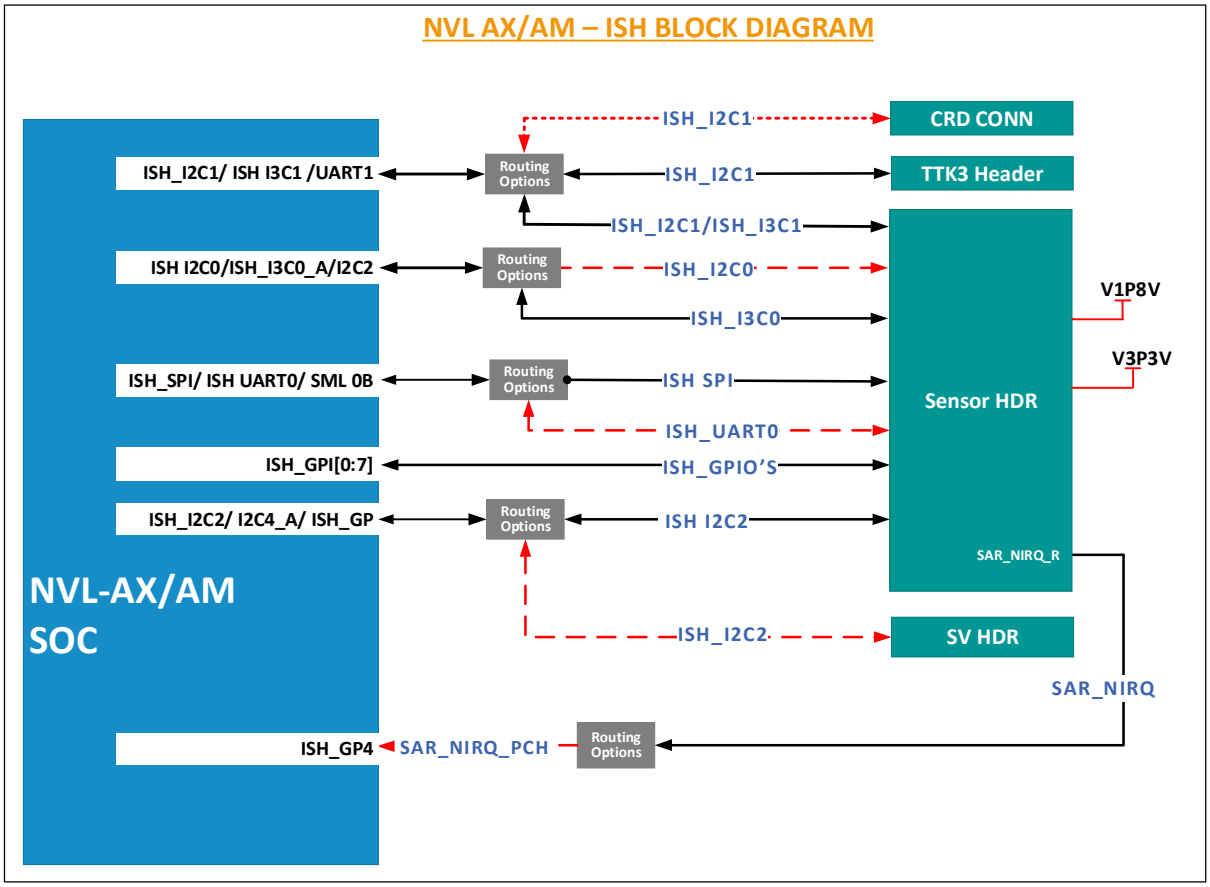


Figure 14-1: NVL AX/AM RVP ISH Sensor Header High level block diagram

14.7. ISH I2C/I3C

The ISH supports three I2C controllers capable of operating at speeds up to 1 Mbps each.

The ISH's I2C host controllers also share the same general I2C port specifications:

- Master Mode Only (all peripherals must be slave devices)
- Support for the following operating speeds:
  - Standard mode: 100kbps
  - Fast Mode: 400kbps
  - Fast Mode Plus: 1Mbps

ISH I3C signal is muxed with ISH I2C.

14.8. ISH UART

ISH supports 2 UART ports capable of supporting operating speeds up to 4 Mbps. ISH UART is used to trace the log output. All the signals are routed to the sensor header.

14.9. ISH SPI

The ISH supports one SPI controller comprises of four-wired interface connecting the ISH to external sensor devices and port is routed to sensor header. The frequency range with a maximum rate of 24Mbps

14.10. ISH GPIOs

ISH GPIO's are typically used for enabling power to the sensor, detecting the interrupts from sensors etc. External pull ups will be provided for ISH GPIOs. Up to 7 dedicated GPIOs can be used from ISH.

14.11. ISH Header

NVL will use the MoSAIC Gen2 board. Modular Sensor Add-In-Card (MoSAIC) Gen 2 is an add-in card to enabling connecting different sensors to sensor-enabled platforms. Its main purpose is to connect sensors to ISH (Integrated Sensor Hub aka ISS, Intel Sensors Solution), but it can be used with other sensor solutions as well. MoSAIC Gen2 is a carrier card which means that no sensors are installed on MoSAIC itself. Instead, the MoSAIC Gen 2 card provides 15 DIP sockets, into each a 1-sensor card with one or more sensors can be plugged. Several switches soldered on the MoSAIC Gen2 board are used to route the sensor signals (I2C/SPI/UART/GPIO) to relevant platform (ISH) pins.

Refer this Wiki link for ISH Header connector Pinout:
https://wiki.ith.intel.com/pages/viewpage.action?pageId=1956229696

Note: the pullup voltage provided by the NVL RVP on pin 1 and 3 is 1.8V only. There is no support for 3.3V on these pins.

14.12. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

15. Touchscreen & Touchpad

15.1. Overview

NVL AX/AM RVP will have two 1x20 Headers on board to support 2 touch panels. These panels will support dual screen. Users can connect two screens to one RVP and have touch and pen work for both panels.

NVL RVP shall support I2C based touch screen by default and SPI based touch with rework on Touch Panel Connector 0. Touch panel 2 will be enabled by THC I2C and THC SPI via rework where THC I2C will be default connected to Touch-Pad connector.

The above-mentioned is the desired default BKC configuration, which shall be configured in BIOS. The ability to switch the I2C/GSPI/THC ports shall be supported in BIOS and configuration can be changed by user preference

The default power gating option is not provided for the POR touch panel as idle power requirement is on the low.

15.2. Human Input domain platform MRD/PRD

Below is the platform MRD/ PRD for the Human input domain.

- Platform MRD HSD link.
- Human Input Domain platform PRD HSD link.

15.3. Human Input domain RVP LZ/ PRD

TBD

Refer the table below for NVL RVP Landing Zone for Human Input.

Table 65: RVP LZ for Touch support on NVL RVPs

Si#	Feature /Interface	RVP
1	**Touch Panel HDR 1 (SPI/ THC/ I2C)**	Yes
2	**Touch Panel HDR 2 (SPI/ THC/ I2C)**	Yes
3	**Touch Pad HDR (THC_I2C / I2C)**	Yes

15.4. HW BOM

The table below gives the list of Modules supported on NVL RVP SKUs for Touch.

Table 66: List of POR modules supported for Touch

Si#	HW BOM Description	Part#/ IPN	Vendor
1	**THC Based Touch panel Display**	THC SPI BOM52	IVO
2	**I2C Based Touch panel Display**	THC I2C BOM 52	IVO
3	**Touch Panel**	Wacom G16T	Wacom
4	**Touch-Pad**	THAT 13T	THAT

15.5. Touchscreen & Touchpad High Level block diagram

The figure below shows the high-level block diagram for touch implementation on NVL RVP.

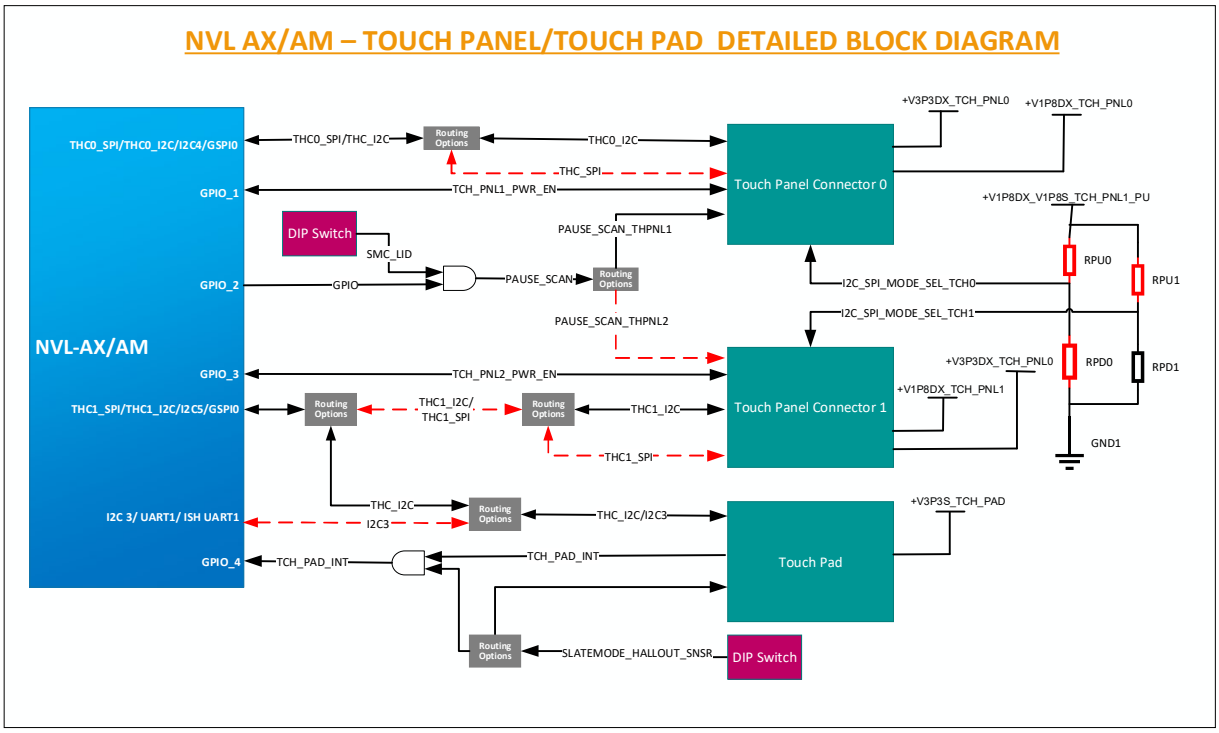


Figure 15-1: Touch Panel & Touchpad detailed level block diagram(TBD)

15.6. Touchscreen

For POR the default interface is 1.8V I2C interface and following signals from SOC/PCD are used as reset and interrupt.

Table 67: Reset and interrupt used for Touchscreen

Si#	GPIO	Function	Description	Voltage
1	TCH_PNL_RESET	Reset	HIGH: Out of Reset LOW: In Reset	PCD I/O voltage (No board level shifting)
2	TCH_PNL_INT	Interrupt	HIGH: No interrupt LOW: Interrupt	PCD I/O voltage (No board level shifting)

Please refer the wiki link for the pinout details for the Touchscreen Header:
https://wiki.ith.intel.com/display/ITSDesignWiki/Touch+Panel+Connector

15.7. Touchpad

NVL RVP provides a 1x12 pin header to interface the THAT based click pad (TBD). The Touchpad interfaced to THC-I2C1 port at 3.3V through the level shifter on board. A rework option is provided from LPSS I2C-3 when THC-I2C1 port functions as Touch Panel.

Please refer the wiki link for the pinout details for the Touch-Pad Header:
https://wiki.ith.intel.com/display/ITSDesignWiki/Touch+Pad+Connector

Note: The 5V will be removed from NVL Touchpad connector. This is no longer used in latest touch pad. So, pin 8 and 9 will NC from PTL onwards.

15.8. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

16. Low Power Sub Systems (LPSS)

16.1. Overview

LPSS is the Low Power I/O Sub-System, which provides a configurable set of external serial I/O ports supporting industry-standard I/O protocols: I3C, I2C, UART, and GSPI. Initial assignment of LPSS port is given in the block diagram of the respective sub-sections.

16.2. LPSS domain platform MRD

Below are the platform MRD for the LPSS domain.

- Platform MRD HSD link.

16.3. LPSS domain RVP LZ/PRD

TBD

Refer the table below for NVL AX/AM RVP Landing Zone for LPSS.

Table 35: RVP LZ for LPSS on various NVL AX/AM RVPs

Sl#	Feature /Interface	NVL-AX/AM RVP
1	**I3C (Debug BPK I3C)**	
2	**I2C0/ I3C0**	Camera con CRD2
3	**I2C1/ I3C1**	Camera con CRD1
4	**I2C2/I3C2**	TBD
5	**I2C3/ UART1**	PSS/ Audio/ Power meter/ Track PAD/ I2C/ SMBUS IO Expander - PCIe Slots, FRU EEPROM, MIPI 60 HDR etc.
6	**THC 0/ GSPI 0/ I2C4**	Touch Panel Con 1 (I2C & THC mode)
7	**THC 1/ GSPI 1/ I2C 5**	Touch Panel Con 2 (I2C & THC mode)
8	**UART 0**	Serial Debug console (uUSB)
9	**UART2/ CNVi BRI/RGI**	M.2 BT integrated and discrete module
10	**MFUART 2**	M.2 WLAN MFUART

16.4. HW BOM/ AIC Details

Refer respective section of this document for HW BOM/AIC details for LPSS.

16.5. I2C/I3C

The SOC implements 6 I2C controllers for 6 I2C interfaces (I2C0-I2C5), capable of maximum bit rate of 3.4 Mbps (High-speed mode). Each interface is a two-wire serial interface consisting of a serial data line (SDA) and a serial clock (SCL). The following are the constraints considered for I2C mapping:

1. Camera sensors and touch screen / touch pad cannot be on the same I2C bus.
2. Each camera connector needs a separate I2C bus to avoid address conflict since all the camera sensors have same I2C address.

Each I2C interface can support the following Speed & power options:

- Standard mode (up to 100 kbps)
- Fast mode (up to 400 kbps)

- Fast mode plus (up to 1 Mbps)
- High speed mode (up to 3.4 Mbps)
- 1.8V support only

NVL supports 4- I3C interfaces with Data Rate (SDR) 12.5 Mbps, Dual Data Rate (DDR) 25 Mbps.

Below image shows high level block diagram of LPSS implementation on NVL AX RVP SKUs.

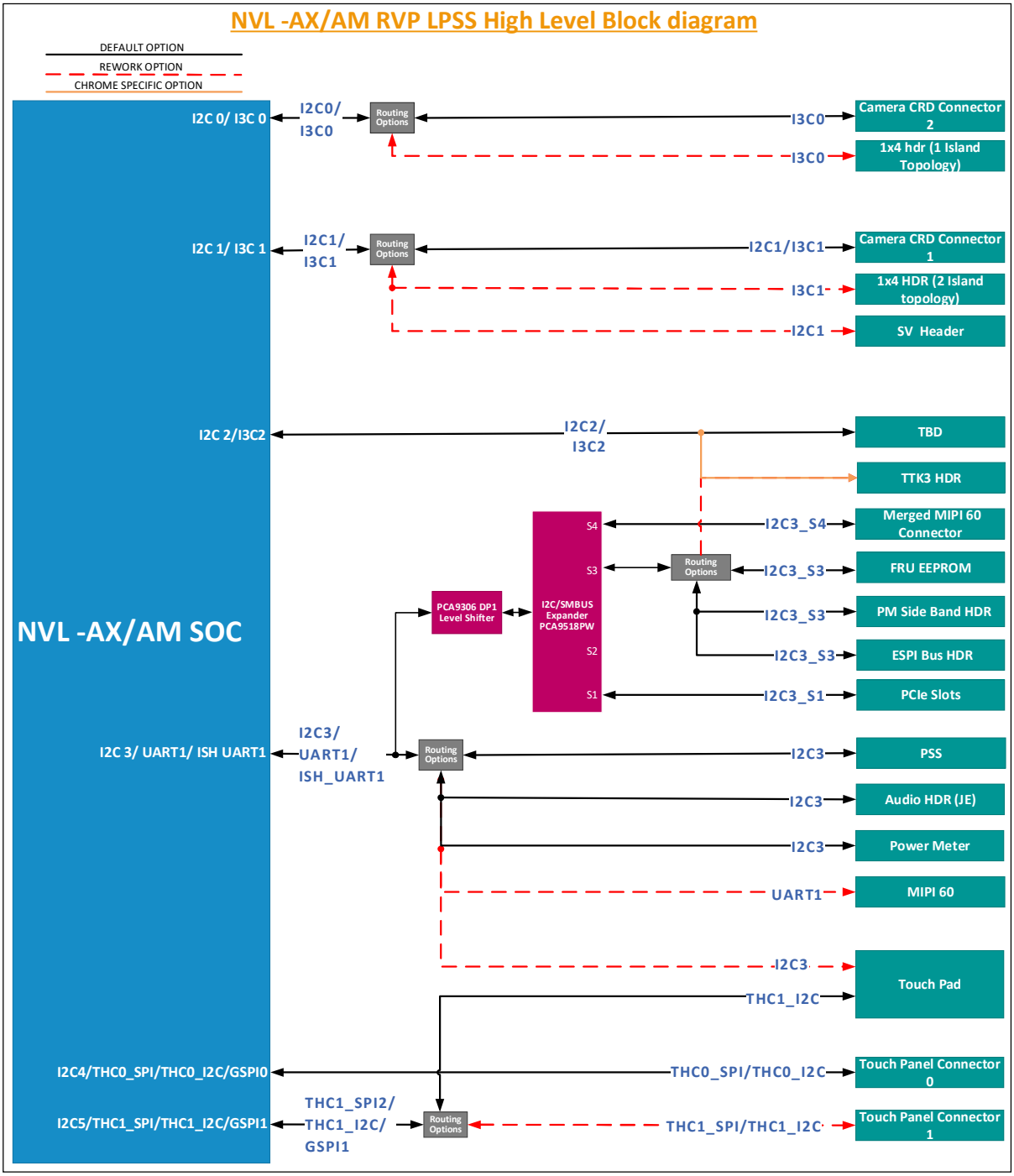


Figure 16-1:LPSS High Level Block Diagram

16.5.1. I2C Device Details

Below table captures the devices that are connected to the LPSS I2C/I3C subsystem

Table 68: I2C/I3C device details (TBD)

Si#	Device	Speed	7 Bit address set	7 Bit address Options	I2C IO Voltage
1	**Touch Pad**	400KHz/1MHz	0x2C	0x2C	3.3V
2	**Touch Panel-2**	400KHz/ 1MHz	0x5C (General Study)	0x5C	1.8V
3	**Touch Panel-1**	400KHz/ 1MHz	0x5C (General Study)	0x5C	1.8V
4	**Cam_Connector-1**	400KHz	0x4D	0x4D	1.8V
5	**Cam_Connector-2**	400KHz	0x49	0x49	1.8V
6	**PSS**	400KHz	0x6E	0X68 or 0x6A or 0X6C or 0X6E	1.8V
7	**Power meter Chip#1**	100KHz/ 400KHz/ 1MHz (FM+)	0X18	Configurable through resistor	1.8V
8	**Power meter Chip#2**	100KHz/ 400KHz/ 1MHz (FM+)	0X1E	Configurable through resistor	1.8V
9	**Power meter Chip#3**	100KHz/ 400KHz/ 1MHz (FM+)	0X11	Configurable through resistor	1.8V
10	**Power meter Chip#4**	100KHz/ 400KHz/1MHz (FM+)	0X15	Configurable through resistor	1.8V
11	**Power meter Chip#5**	100KHz/ 400KHz/1MHz (FM+)	0X19	Configurable through resistor	1.8V
12	**Power meter Chip#6**	100KHz/ 400KHz/1MHz (FM+)	0X17	Configurable through resistor	1.8V
13	**Power meter Chip#7**	100KHz/ 400KHz/1MHz (FM+)	0X12	Configurable through resistor	1.8V
14	**Power meter Chip#8**	100KHz/ 400KHz/1MHz (FM+)	0X1D	Configurable through resistor	1.8V
15	**Power meter Chip#9**	100KHz/ 400KHz/1MHz (FM+)	0X1A	Configurable through resistor	1.8V
16	**Power meter Chip#10**	100KHz/ 400KHz/1MHz (FM+)	0X1B	Configurable through resistor	1.8V
17	**Power meter Chip#11**	100KHz/ 400KHz/1MHz (FM+)	0X13	Configurable through resistor	1.8V
18	**FRU EEPROM**	100KHz/400KHz	0xAD (Read), 0xAC (Write)	Configurable through resistor	3.3V

Note: The number of power meters used on the platform and slave address are TBD.

16.6. UART

The LPSS Subsystem includes 3 UART ports. The UART ports communicate with serial data port devices compatible with the RS-232 interface protocol. The device mapping for the LPSS-UART interfaces on NVL AX/AM RVP SKUs are as shown below. For detailed implementation of USB to UART BRIDGE IC, kindly refer to section 26.8.4.4.

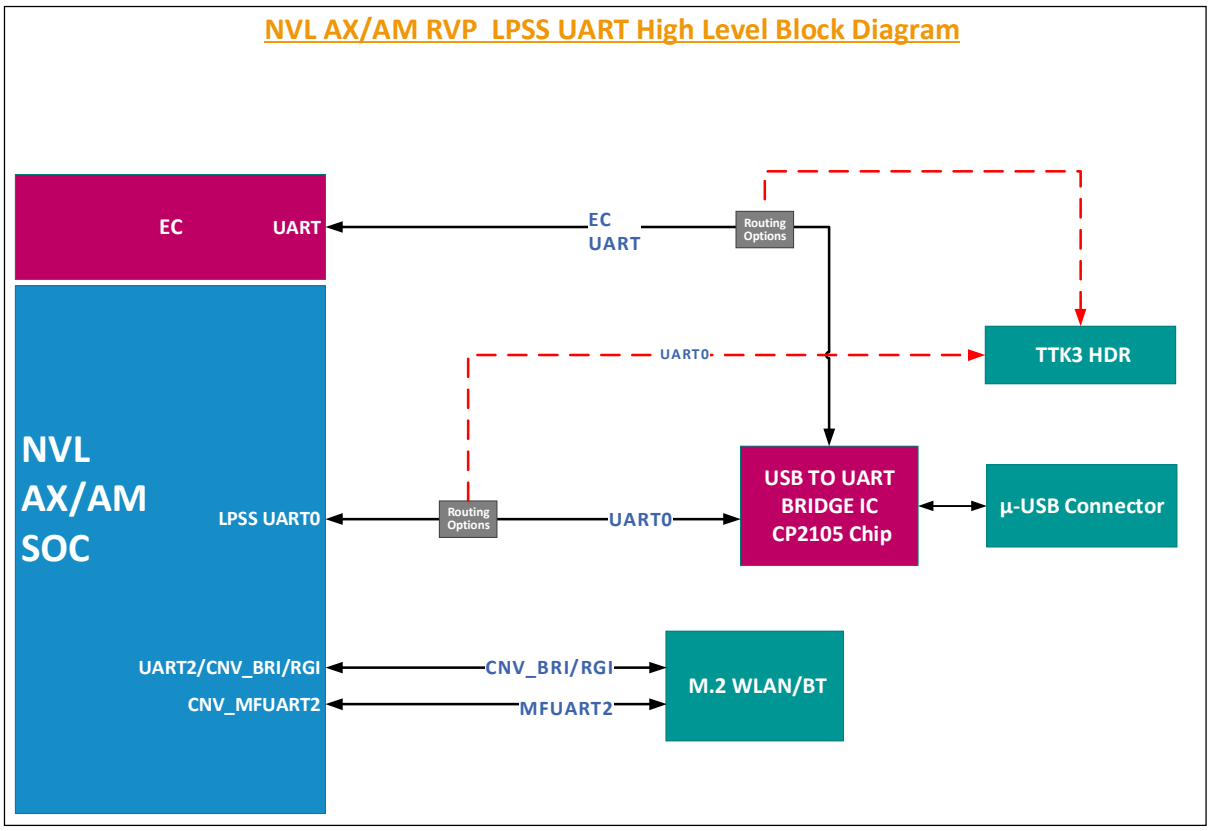


Figure 16-2: NVL AX/AM RVP LPSS UART High Level Block Diagram

16.7. GSPI

There is no dedicated header in NVL AX/AM RVP for GSPI. GSPI[1:0] signals are Multiplexed with THC SPI[1:0] signals, but THC is POR for NVL AX/AM RVPs. NVL AX/AM RVP supports GSPI based Fingerprint Sensor via rework only over GSPI2 port.

16.8. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

17. Serial Interfaces- SPI, eSPI, SM Link, MLink/ CLink

17.1. Overview

This chapter discusses about the various serial interfaces namely SPI, eSPI, SMLink, MLink. The SPI and eSPI functionally similar IPs. The mapping of all serial ports is as shown below. The mapping is subjected to change based on the inputs from design or validation teams.

17.2. Serial Interface domain platform MRD/PRD

Below are the platform MRD/ PRD for the Serial Interfaces.

- Platform MRD HSD link.
- Serial Interface domain platform PRD HSD link

17.3. Serial Interface domain RVP LZ

Refer respective section of this document for Serial Interfaces Landing Zone on NVL RVP.

Table 69: RVP LZ Serial Interfaces for NVL

Si#	Feature /Interface	RVP01
1	**SML 0**	Jackson Ville/ Foxville AIC (PCIe x1 slot)/ dTBT BR AIC (x4 slot)/Integrated TBT
2	**SML 1**	Sideband HDR/ EC
3	**USBC_SML**	dTBT BR AIC (x4 slot)/Integrated TBT /EC/Sideband HDR
4	**OSSE_SML**	No POR end point device
5	**SMBUS (removed from NVL onwards - replaced with LPSS I2C2)**	NA, Not POR from NVL platform onwards

17.4. HW BOM/ AIC Details

Refer the individual chapters for HW BOM/AIC details of Serial Interfaces.

17.5. SPI & eSPI Ports

The NVL SOC provides Serial Peripheral Interfaces (SPI) for connecting BIOS Flash, TTK3 and TPM. Which is 1.8V IO voltage only with maximum speed of 100MHz.

The SPI0 (CSME SPI) interface consists of 3 chip-select signals. It is allowing up to two flash memory devices (SPI0_CS0# and SPI0_CS1#) and one TPM device or TTK3 device (SPI0_CS2#) to be connected to the SOC working in quad-mode. The SPI0 interfaces support 1.8V only.

The PCD – H eSPI (Enhanced SPI) controller supports the following features:

- Support for 20MHz, 25MHz, 33Mhz and 50MHz bus operation.
- 1.8V support only
- Support for PCH.IOE on eSPI CS#3
- Up to quad mode support with 2 Chip Select signals.

Refer to the chapter 15 BIOS Flash Interface (SPI) section for detailed explanation on the Flash sharing mechanisms and eSPI Interface.

For SPI: Refer BIOS Flash Interface section.

For eSPI: Refer eSPI section.

17.5.1. PCH-IOE SPI port

There is no Flash sharing between PCD-H and PCH-IOE. NVL RVP supports a dedicated PCH-IOE SPI port for 8MB SPI Flash device for PCH-IOE FW.

Below is the SPI high level block diagram.

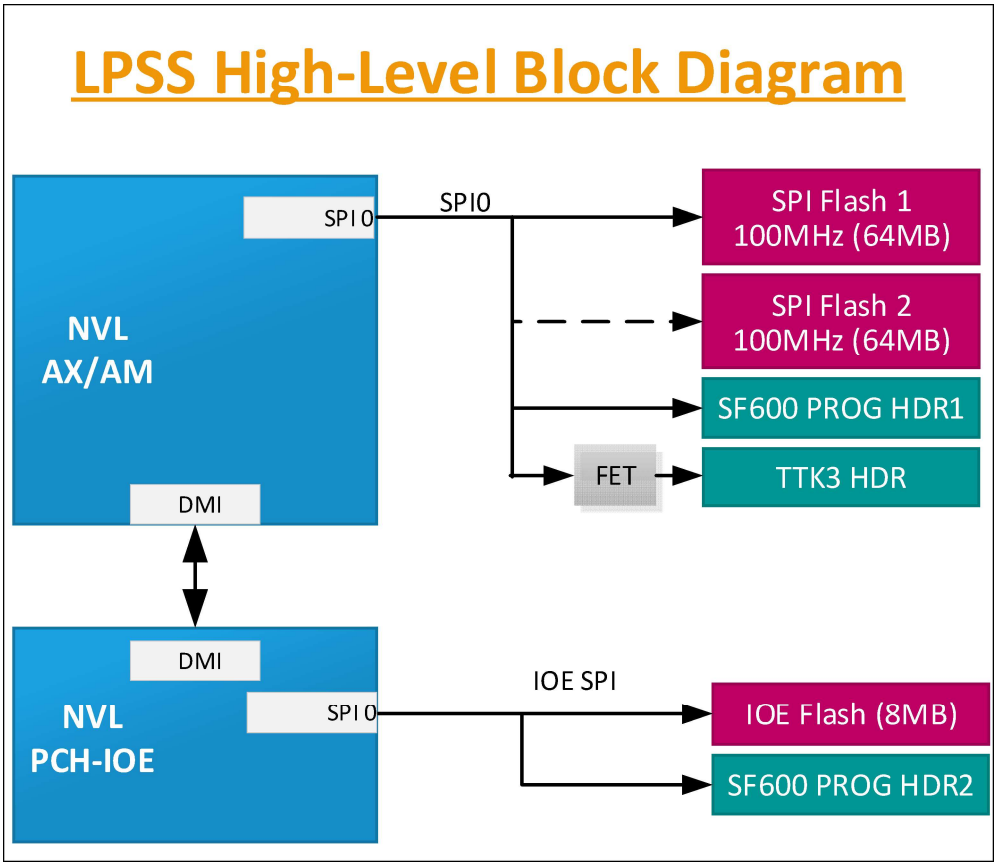


Figure 17-1: SPI High level Block Diagram

17.6. SMLink

NVL AX/AM SoC implements 2 SMLink controllers for the 3 SMLink interfaces, SMLink0, SMLink0B and SMLink1. The interfaces are intended for system management and are controlled by the Intel® ME. And they can run at frequencies up to 1MHz.

- SMLink0 is mainly used for integrated LAN. When an Intel LAN PHY is connected to SMLink0, a soft strap must be set to indicate that the PHY is connected to SMLink0. The interface will be running at the frequency of up to 1 MHz depending on different factors such as board routing or bus loading when the Fast Mode is enabled using a soft strap.
- SMLink1 is kept as routing option to PD Controllers and PM Sideband Header
- SMLink0B is muxed with ISH UART0/ISH_SPI and default used as ISH UART0
- USBC_SML is routed to PD Controller and PM Sideband Header
- OSSE_SML is used as GPIO's

Note: *SMBUS is no longer supported from NVL onwards and replaced with LPSS I2C2*

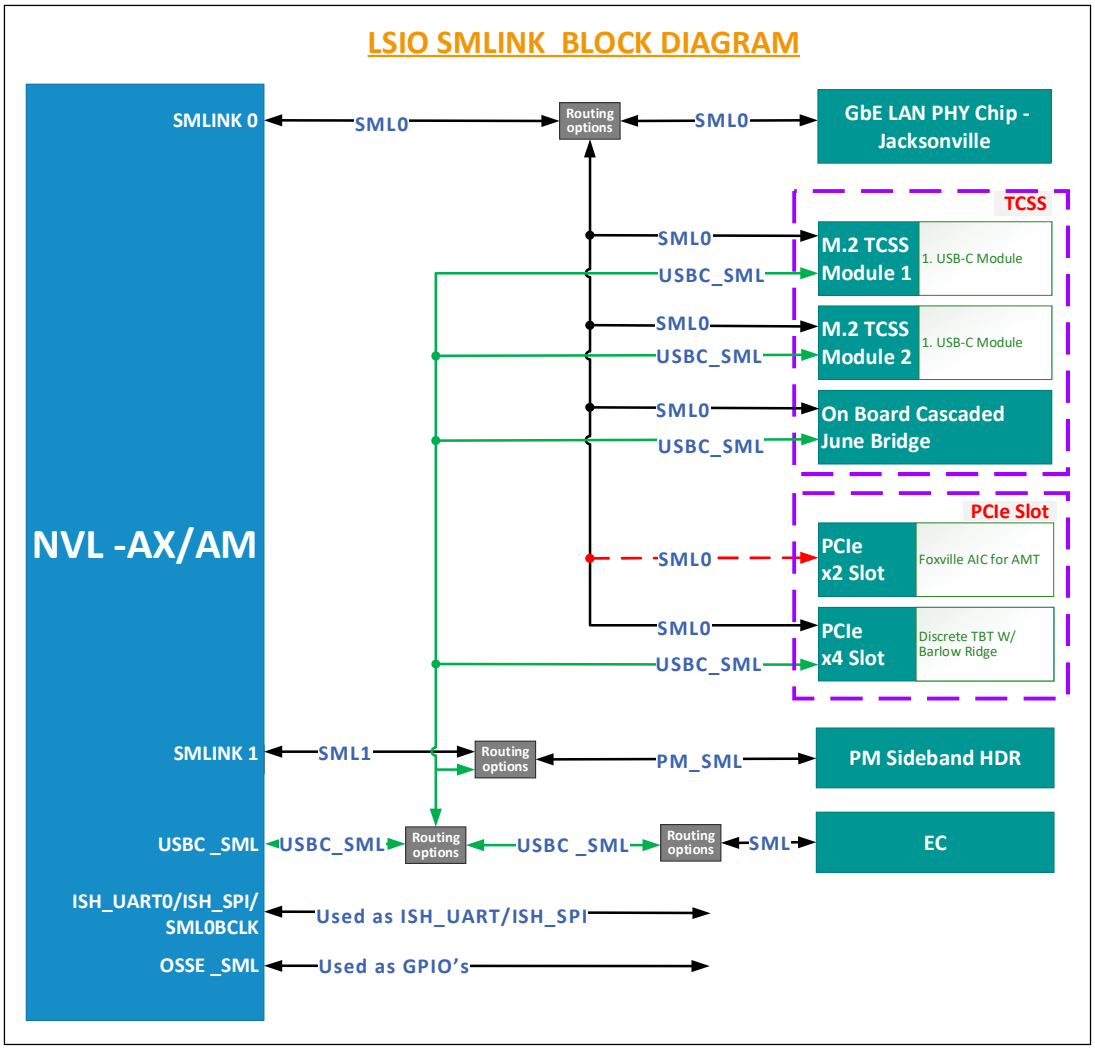


Figure 17-2: NVL RVP SMLink High Level Block Diagram (TBD)

17.7. MLink / Clink

M-Link interface is the management communication link between the SOC and Intel Wireless cards. It enables Manageability to support low power interface of Intel WiFi network interfaces. The signal routing option is provided through a tri-pad, to the WLAN module, 2x4 Header and SOC.

Note: Clink has also been called Manageability link (MLink) in some documentation.

Table 70: CLink Interface Signals

Si#	Signal Name	Type	Description
1	CL_RST#	O	Wi-Fi* CLINK host bus reset for standard CNV with CLINK support (Intel® vPro™). Optional to connect to a Wi-Fi* CLINK reset pin on the Intel® vPro™ Wi-Fi* module.
2	CL_DATA	I/O	Wi-Fi* CLINK host bus data for standard CNV with CLINK support (Intel® vPro™). Optional to connect to a Wi-Fi* CLINK data pin on the Intel® vPro™ Wi-Fi* module.
3	CL_CLK	O	Wi-Fi* CLINK host bus clock for standard CNV with CLINK support (Intel® vPro™). Optional to connect to a Wi-Fi* CLINK clock pin on the Intel® vPro™ Wi-Fi* module.

17.8. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

18. Embedded Controller

18.1. Overview

NVL AX/AM RVP will support MEC1723 Microchip Embedded Controller (EC) onboard. MEC1723 ESPI mode of operation. LPC mode will not be supported in NVL. EC controls the preliminary platform power sequencing and does system and power management. EC is the platform thermal controller that monitors and throttles CPU or controls CPU Fan. The key functionalities of EC on the platform are illustrated in below figure.

Note: EC part (144-pin WFBGA package) used in NVL design is **MEC1723NB0-I/SZ** EC domain platform MRD/PRD

Below is the platform MRD/ PRD for the EC domain.

- Platform MRD HSD link.

18.2. EC domain RVP LZ/ PRD

TBD

Below table capture the EC feature support on NVL RVPs.

Table 71: EC Domain Feature set

Si#	EC domain features	NVL-AX RVP
1	**eSPI based EC support**	Yes
2	**MECC AIC support**	No
3	**EC SM BUS IO Expander - 2 no's**	Yes

18.3. HW BOM

Below table capture the EC HW BOM in NVL RVPs.

Table 72: NVL EC HW BOM

Si#	HW BOM Description	Part#/ IPN	Vendor
1	EC (without I3C support)	MEC1723	Microchip (Mobile)

18.4. BLOCK Diagram

Below is the high-level block diagram for EC implementation on NVL RVP.

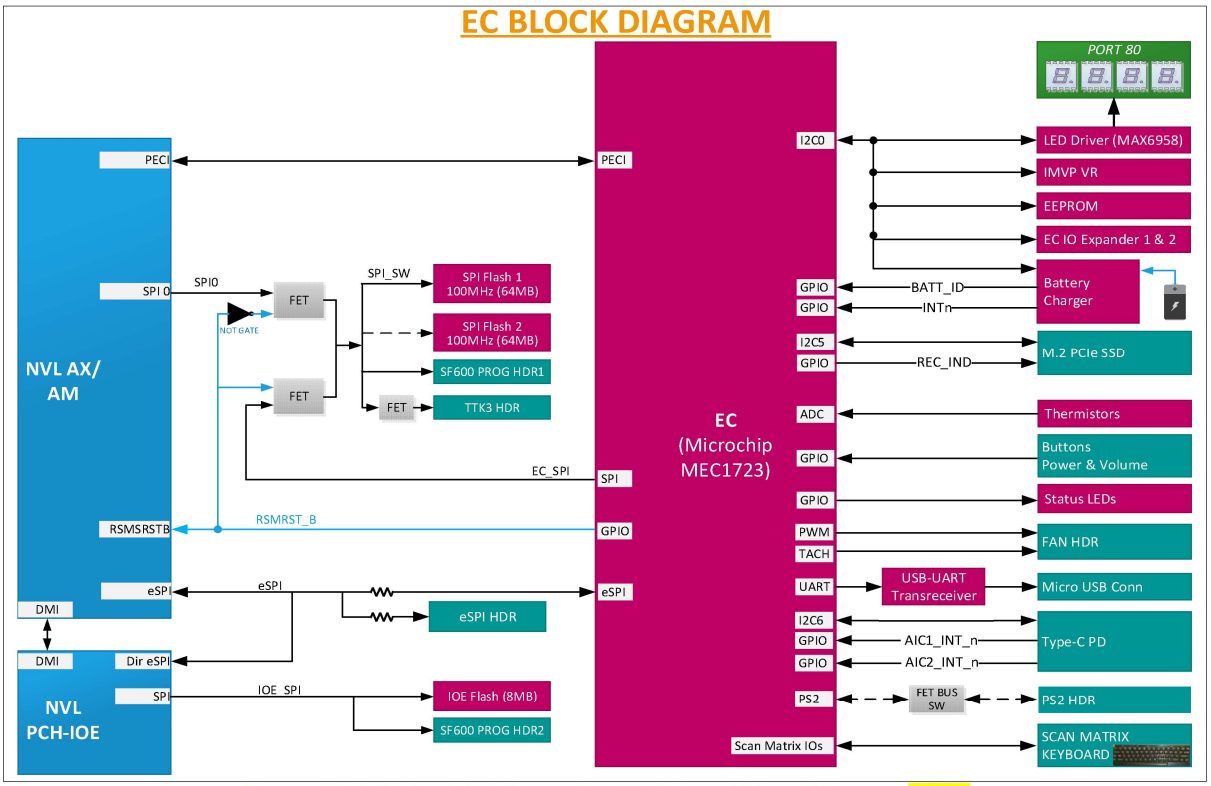


Figure 18-1:Embedded Controller High-Level Block Diagram (TBD)

The EC subsystem consists of:

1. Thermal Management functions like CPU Fan control, Chassis Fan control, PECI temperature etc.
2. Platform Power management like Power sequencing, Sx and S0ix entry/exits.
3. Any CEC specific Modern Standby requirements to be implemented inside EC
4. Handles the Board-ID, Fab-ID, BOM SKU-ID, messages to the BIOS.
5. RVP design will support all three i.e., SAF, MAF, G3 Flash configuration, default will be MAF.
6. 2x14 pin eSPI header will be supported.
7. Switching between MAF / SAF / G3 will be through resistors rework and switch settings change.
8. Separate PMR resistors will be added for 1.8V and 3.3V rails going to EC.
9. EC GPIO mapping Link TBD.

NVL RVP carry forwarding changes/ optimizations done in PTL platform in the EC and MECC sections to ease out the routings, reduce BOM cost, add extra features etc. The details are mentioned below.

1. Only one PS2 header is supported over the NVL RVP which is default configured as PS2 KB from EC. EC has only one PS2 IP which can be configured as PS2 KB/ PS2 mouse at any given point of time. This PS2 KB header is only stuffed in NVL RVP.
2. The LDO to generate the VREF ADC rail has been removed in NVL RVP as in PTL RVPs. So, this is generated from 3.3VA KBC EC rail in current design (same as VTR_PLL rail, as recommended in EC datasheet).
3. There are 3 additional thermistors (ET THERM1, ET THERM2, ET THERM3) in NVL RVP getting mapped to the EC for energy telemetry application.
4. EC EEPROM is removed from NVL RVP as deep Sx state is not supported in none of the SKUs.
5. Few signals are removed from the on-board EC due to lack of functionality to ease out the routing (EC SMI signal, HB NVDC SEL, EC SLP S0 CS, INT from board ID IO expander, Aux adapter detect, EC SML CLK/ DATA).

The RVP supports LED for CAPSLOCK, NUMLOCK and SCROLL LOCK. The EC error code table with on-board LED status is given below.

Table 73: EC error code indication

Error type	Error code	Caps Lock LED	Scroll Lock LED	Num Lock LED
No Error	0	Off	Off	Off
RSMRST#_PWRGD	1	Off	Off	Flash
PM_SLP_S5#	2	Off	Flash	Off
PM_SLP_S4#	3	Off	Flash	Flash
PM_SLP_S3#	4	Flash	Off	Off
PM_SLP_A#	5	Flash	Off	Flash
ALL_SYS_PW_RGD	6	Flash	Flash	Off
PLTRST#	7	Flash	Flash	Flash
Thermal Shutdown	-	Blink Alternately	-	Blink Alternately

It is to be noted that,

1. KSC Thermal Shutdown is indicated by flashing of Num_Lock and Caps_Lock LEDs alternatively.
2. The above errors are displayed by EC on Port80 as EC 01 to EC 07. These errors are not EC errors, and these errors represent the platform status. For Thermal Shutdown there is no Error code.

18.5. MECC AIC Support

No MECC AIC Support on NVL-AX/AM RVP

18.6. eSPI

NVL PCD-H supports 1 eSPI interface with below features:

1. 1.8V I/O, supporting single, dual and quad I/O mode.
2. Support 20 MHz, 25 MHz, 33 MHz, and 50 MHz bus operation.
3. Support in-band ALERTB for single chip select configuration.

NVL AX/AM RVP supports 2 load eSPI topology with EC as 1st load and PCH-IOE as 2nd load.
NVL RVP 05/06 supports 1 load eSPI topology with EC as 1st load
Below is the high-level block diagram for eSPI implementation in NVL RVP.

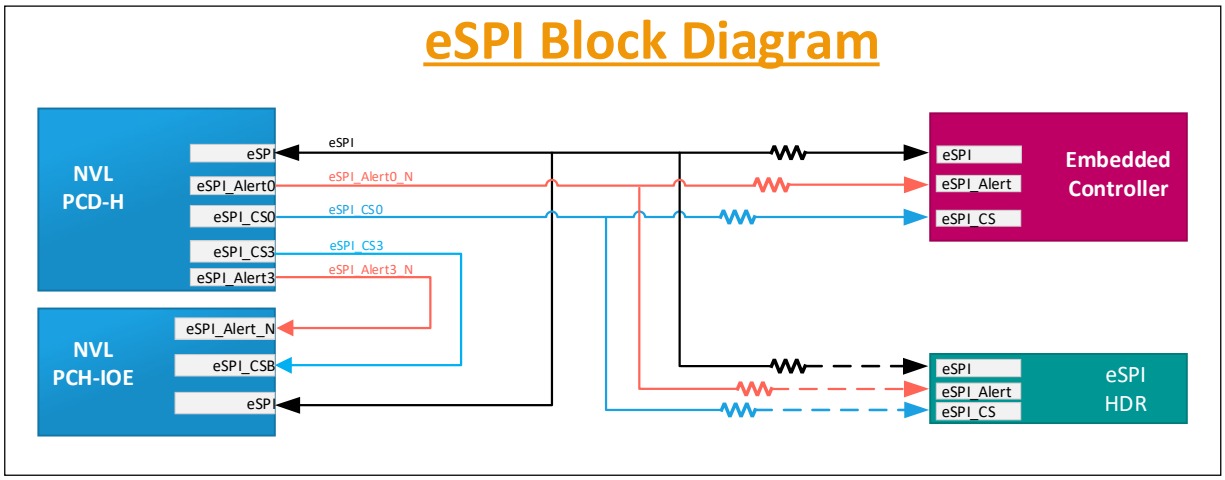


Figure 18-2: eSPI High Level Block Diagram (TBD)

18.7. Features

18.7.1. Flash Sharing

NVL RVP supports all MAF, SAF and G3 flashing configuration. There is no dedicated Flash to EC. SOC GPIO is used for flash selection strap pin refer (Pin strap section link TBD) for more details refer to SOC/EC SPI Flash Section.

EC shared flash (SOC SPI NOR).

1. Shared SPI Flash: Currently a Composite image. Update is done by BIOS. Top swap allows recovery.

18.7.2. EC – I2C and IO Expander

I2C based IO expanders are provided to handle Board-ID, Fab-ID, BOM SKU-ID and some IO requirement. EC I2C mapping is provided in the below figure.

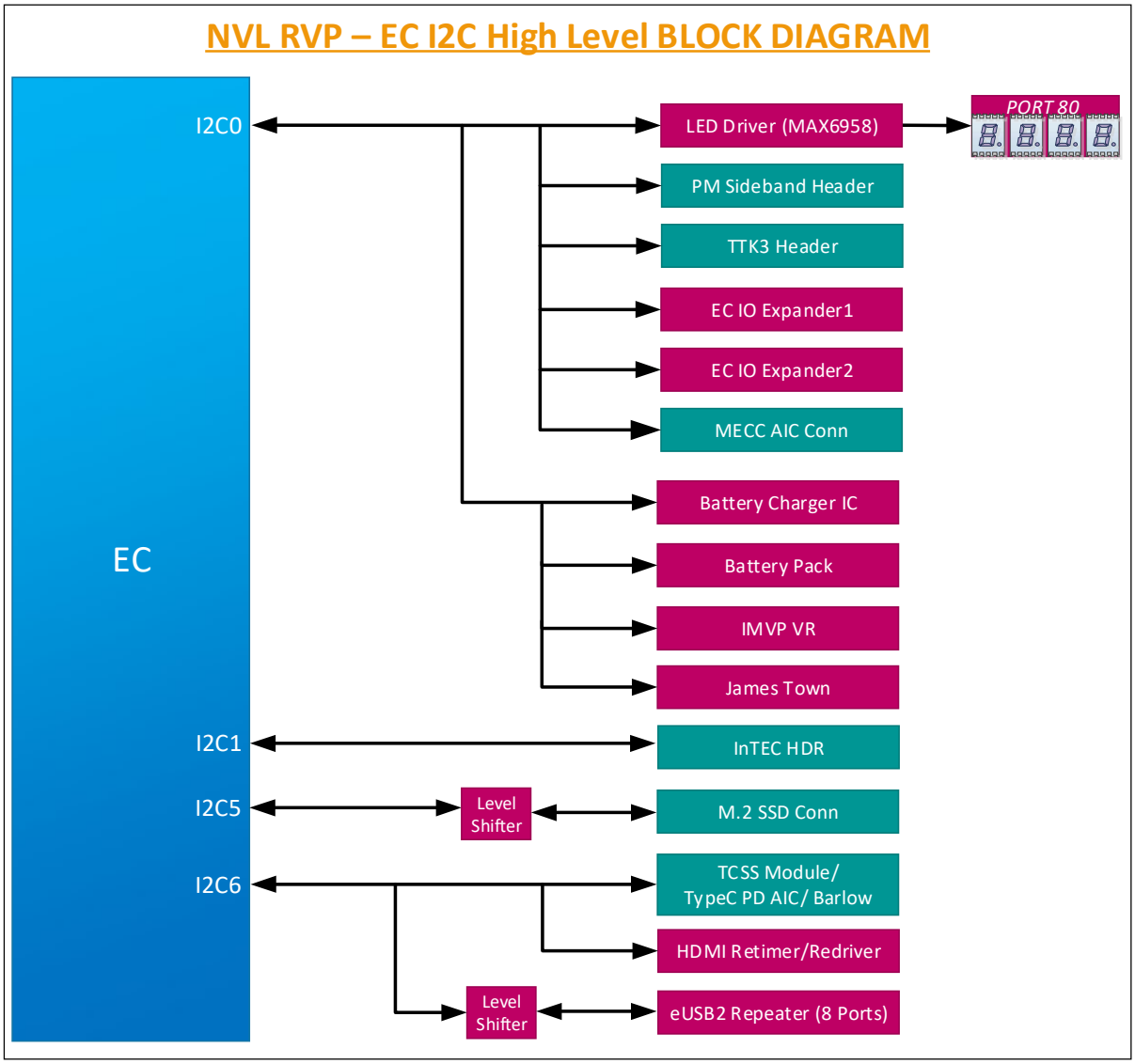


Figure 18-3: EC- I2C and IO Expander High Level Block Diagram

18.8. EC – Headers

Below sections includes connector and pinout details of the connectors used in EC section.

18.8.1. eSPI Sideband Header

Note: In NVL RVP, Glider card KOZ support is removed (from PTL onwards). eSPI Header will be supported with Feature rework option similar to previous platforms.

Below table capture the eSPI Header and Pinout supported on NVL RVPs.

Table 74: eSPI Sideband Header

MFG	Mfg. Part Number	IPN Number
Samtec	ASP-175166-01	H46981-001

Table 75: eSPI Sideband Pinout

Signal Name	Pin #	Pin #	Signal Name
ESPI_CLK_HDR	1	2	GND
ESPI_CS0_HDR_N	3	4	NO PIN
SHM_TRIG_PLT_RST_R	5	6	+V5A_VAL
ESPI_IO3_HDR	7	8	ESPI_IO2_HDR
+V3P3A_VAL	9	10	ESPI_IO1_HDR
ESPI_IO0_HDR	11	12	GND
SMB_CLK_S3	13	14	SMB_DATA_S3
+V3.3A_1.8A_R1_TPM	15	16	ESPI_CS1_HDR_N
GND	17	18	ESPI_CS2_HDR_N
ESPI_RST_HDR_N	19	20	ESPI_ALERT0_HDR_N
NO PIN	21	22	NO PIN
ESPI_ALERT1_HDR_N	23	24	ESPI_CS3_HDR_N
TP_GPP_A8_CLKRUN_R_N	25	26	ESPI_ALERT3_HDR_N
+V5A_VAL	27	28	ESPI_ALERT2_HDR_N

18.8.2. PS2 KB HEADER

Below table capture the PS2 KB Header and Pinout supported on NVL RVPs.

Table 76: PS2 KB Header

MFG	Mfg. Part Number	IPN Number
SAMTEC/ Weison	TSM-105-01-L-SV-P-TR/ AC2100-0009-070-HH	J47721-001

Table 77: PS2 KB Header and Pinout

Pin #	Signal Name
1	PS2_KB_CLK_FB
2	+V5_PS2
3	GND
4	GND
5	PS2_KB_DATA_FB

18.8.3. PS2 Mouse HEADER

There is no PS2 mouse header on NVL RVP. We have only one PS2 header which is configured as PS2 KB from EC. This support is removed from PTL-UH RVP onwards.

18.8.4. Scan Matrix Keyboard Header

Below table capture the Scan matrix Keyboard Header and Pinout supported on NVL RVPs.

Table 78: Scan Matrix Header

MFG	Mfg. Part Number	IPN Number
Ipex	20542-028E-01	H24635-001

Table 79: Scan Matrix Pinout

Pin #	Signal Name
1	KBC_SCANIN<6>
2	KBC_SCANIN<0>
3	KBC_SCANIN<1>
4	KBC_SCANOUT<6>
5	KBC_SCANIN<3>
6	KBC_SCANIN<2>
7	KBC_SCANOUT<15>
8	KBC_SCANIN<5>
9	KBC_SCANIN<4>
10	KBC_SCANOUT<10>
11	KBC_SCANOUT<14>
12	KBC_SCANIN<7>
13	KBC_SCANOUT<13>
14	KBC_SCANOUT<11>
15	KBC_SCANOUT<8>
16	KBC_SCANOUT<7>
17	KBC_SCANOUT<9>
18	KBC_SCANOUT<12>
19	KBC_SCANOUT<3>
20	KBC_SCANOUT<2>
21	KBC_SCANOUT<1>
22	KBC_SCANOUT<4>
23	KBC_SCANOUT<5>
24	KBC_SCANOUT<0>
25	LED_NUMLOCK
26	LED_CAPSLOCK
27	+V3.3A_KBC
28	NC

18.8.5. Keyboard Backlight Header

Below table capture the Keyboard Backlight Header and Pinout supported on NVL RVPs.

Table 80: KB Backlight Header

MFG	Mfg. Part Number	IPN Number
Ipex	20542-006E-01	H24575-001

Table 81: KB Backlight Pinout

Pin #	Signal Name
1	+V5S_KBD_BKLT
2	+V5S_KBD_BKLT
3	NC
4	NC
5	KBD_BKLT_CTRL_FET
6	KBD_BKLT_CTRL_FET

18.8.6. Fan Header (TBD)

Below table capture the FAN Header and Pinout supported on NVL RVPs.

Table 82: Fan Header

MFG	Mfg. Part Number	IPN Number
Molex	53398-0471	K97577-001

Table 83: Fan Header Pinout (Fan part TBD 12V/5V)

Pin #	Signal Name
1	CPU_PWM_FAN
2	CPU_TACH_OUT
3	GND
4	+V5A_PWM_FAN

18.9. Front Panel Header

Below table capture the Front Panel Header and Pinout supported on NVL RVPs.

Table 84: Front Panel Header

MFG	Mfg. Part Number	IPN Number
WIESON TECHNOLOGIES CO., LTD	AC2100-0009-042-HH	K96810-001

Table 85: Front Panel Pinout

Signal Name	Pin #	Pin #	Signal Name
FRONT1(Pull up to 5V)	1	2	FRONT2 (Pull up to 5V)
TP_NC	3	4	GND
GND	5	6	PWR_CONN_D
RST_PUSH_N_D	7	8	GND
+V5A_VAL	9	10	No Pin
NC	11	12	GND
GND	13	14	No Pin
BC_ACOK_DSW	15	16	+V5A_VAL

18.10. PM Sideband Header (TBD)

Below table capture the PM Sideband Header and Pinout supported on NVL RVPs.

Table 86: PM Sideband Header

MFG	Mfg. Part Number	IPN Number
Molex	87832-4020	C12536-002

Table 87: PM Sideband Header Pinout (TBD)

Signal Name	Pin#	Pin #	Signal Name
PM_PWRBTN_N	1	2	ALL_SYS_PWRGD
PM_RSMRST_N	3	4	SMB_BS_DATA_PORT80_R
PM_SLP_S5_N	5	6	SMB_BS_CLK_PORT80_R
PM_BATLOW_N	7	8	NC
PM_SLP_S3_N	9	10	SIDEBAND_TIME_SYNC_0
PM_SLP_S4_N	11	12	USBC_SML_DATA_PD_R
+V3P3A	13	14	USBC_SML_CLK_PD_R
EDM_SOC_IOE_PM_HDR	15	16	GND
RTC_RST_N	17	18	EDM_BASE_PM_HDR
SMC_WAKE_SCI_N	19	20	EDM_GCD_PM_HDR
NC	21	22	BC_ACOK_EC_IN
PS_ON_SW_N	23	24	PM_SLP_A_N
M2_SSD_EC_I2C05_CLK	25	26	PM_PCH_PWROK
M2_SSD_EC_I2C05_DATA	27	28	SRTC_RST_N
RECVRY_INDICATOR_N	29	30	RSMRST_PWRGD_N
PM_SYSRST_N	31	32	PM_SLP_S0_N
+V1P8A	33	34	BUF_PLT_RST_N
I2C2_SDA_S3_J	35	36	SYS_PWROK
I2C2_SCL_S3_J	37	38	EDM_CORE_PM_HDR
+V3P3S_VAL_J	39	40	+V3P3S_VAL_J

18.11. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

19. BIOS Flash Interface (SPI)

19.1. Overview

NVL RVP supports native SPI interface SPI0. The SPI0 is for used for SPI flash and TPM while THC SPI1 and THC SPI2 are used for Touch interface.

NVL RVP supports 1.8V, 64MB flash with RPMC on SPI0 interface. No 3.3V SPI support for NVL SOC. RVP will use 1x 64MB parts default (dedicated 100 MHz 64MB flash for fast boot validation). To validate CS1 of SoC, second flash device will be provided as rework option. With Dual flash configuration, the max speed support is limited to 50MHz.

TPM AIC should be plugged into the same header (SF600 Header) used for BIOS flashing.

NVL RVP will support MAF/ SAF and G3 modes.

Jumper for Flash Descriptor Override will be supported. Also, RVP allows to boot the platform while Dediprog SF600/SF100 programmer is connected to the platform. Certain customers will be booting RVP using SPI device emulator connected to TPM connector or TTK connector. While doing this, the onboard SPI Flash will be isolated.

19.2. SPI Flash domain platform MRD/PRD

Below is the platform MRD/ PRD for the SPI Flash domain.

- Platform MRD HSD link.
- SPI Flash Domain platform PRD HSD link.

19.3. SPI Flash domain RVP LZ/ PRD

TBD

Below table capture the SPI Flash features supported on NVL RVPs.

Table 88: SPI Flash Domain Features

Si#	SPI Flash domain features	NVL-AX/AM
1	**SPI capacity (64MB)**	Yes
2	**50MHz Dual Flash support**	Yes (Unstuffed)
3	**100MHz Flash support**	Yes, 1x
4	**Flash Operating Voltage**	1.8V
5	**SPI device Footprint Supported**	Yes
6	**SPI socket provided on RVP**	No
7	**SPI socket KOZ supported**	No
8	**SPI programming SF600 header**	Yes
9	**SPI programming TTK3 header**	Yes
10	**BIOS configure jumper**	Yes
11	**Clear CMOS jumper**	Yes
12	**FRU (Connected to PCH/ PCD)**	Yes
13	**Boot Support**	Yes
14	**BIOS recovery support from NVMe**	Yes, I2C
15	**SPI Flash (8MB) for optional PCH**	Yes

19.4. HW BOM

Below table capture the SPI Flash HW BOM supported on NVL RVPs.

Table 89: NVL SPI FLash HW BOM

Si#	HW BOM Description	Part#/ IPN	Vendor
1	**64MB SPI Flash with RPMC 1.8V @100MHz (Single flash topology)**	1. W25R512NWEIQ 2. MX77U51250F	1. Winbond 2. Macronix
2	**8MB SPI Flash 1.8V for AX/AM optional PCH IOE @ 100MHz**	1. W25Q64JW (TBD) 2. MX25U6432F	1. Winbond 2. Macronix

19.5. BLOCK Diagram

The SPI0 interface of SOC on NVL RVPs is shown in below diagram.

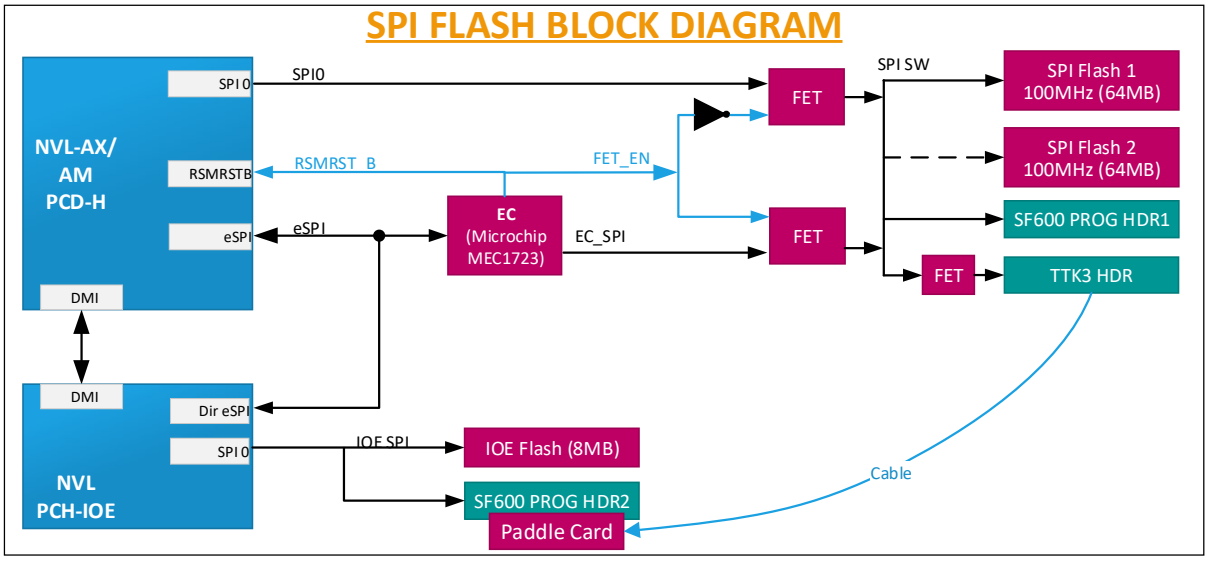


Figure 19-1: BIOS SPI Flash interface (TBD)

19.6. SoC/EC Flash Topology

EC FW image is stored in either external SPINOR or embedded flash. The embedded flash should have enough space to store the entire FW and any Non-Volatile data. ECs without embedded flash requires an external SPI flash, either dedicated or shared with SOC. Three types of flash sharing mechanisms shall be supported on NVL RVP designs.

1. G3 flash sharing
2. MAF - Master attached flash sharing <**default option for platform**>
3. SAF - Slave attached flash sharing.

NVL RVP shall support all flash sharing mechanism. Reworks are required to change into SAF or G3 from MAF.

19.6.1. G3 Flash Sharing

In this mechanism, the SPI lines from flash part are connected to both SOC and EC either directly or switch. Due to security concerns and flash access limitation, this is the least recommended option in all the flash sharing mechanisms.

1. The RSMRST# from EC is used for controlling the flash access and switched only once during G3 exit.

2. EC accesses the SPINOR only when RSMRST# is asserted and tri-states the SPI lines on de-assertion.
3. On G3 exit (with RSMRST# asserted) EC loads the entire image in its internal SRAM and releases RSMRST# for SOC to access the flash. This doesn't require eSPI to be operational.
4. Some isolation FETs required if SOC doesn't tristate the lines when RSMRST# is asserted.

Below is the high-level block diagram for G3 Flash sharing.

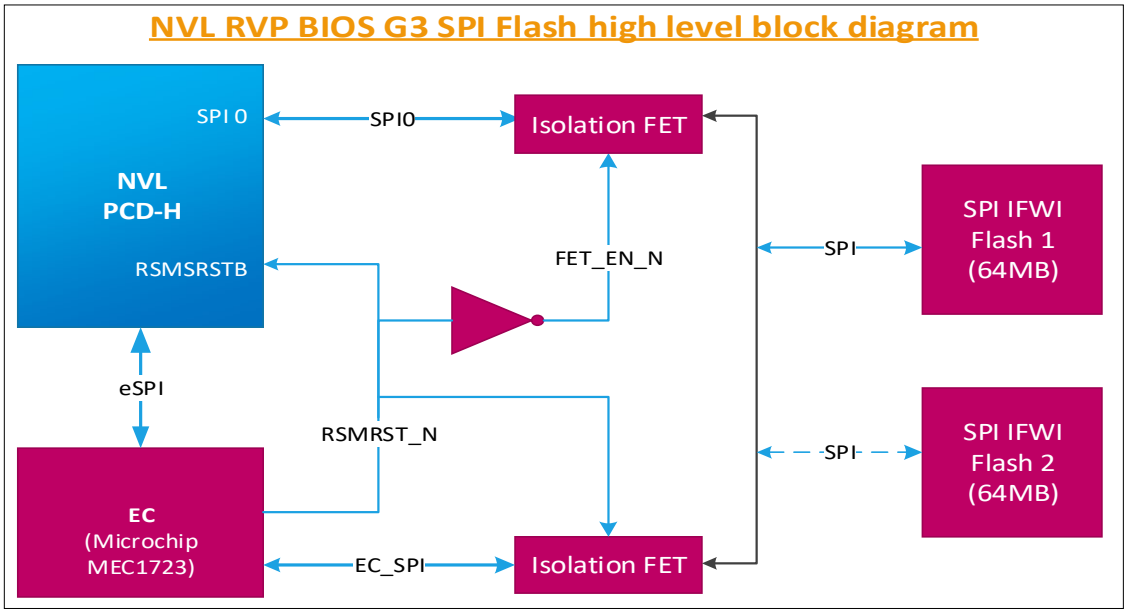


Figure 19-2: G3 Flash Sharing high level block diagram

19.6.1.1. Flash update

1. Requires host to update the EC region in shared SPINOR without EC involvement.
2. Update is like any other OEM regions like BIOS.
3. Host can support Full image update or EC region update.
4. UEFI Capsule update is the minimum requirement with BIOS signature verification.
5. FW recovery
   a) Intel SOC is not responsible for EC FW recovery.
   b) OEMs may support through alternate options
      i) Use other interface that is active in S5 (typically used in service center)
      ii) Implement non updatable block (ROM) in EC that brings up the system to S0 for flash update.

19.6.2. Master Attached Flash Sharing (MAF)

MAF is one of the Flash sharing mechanisms where SOC is the master which access flash over SOC SPI0 Controller and EC sharing same flash will access over eSPI. MAF will be default configuration for NVL.

Here the SPI flash is connected to SOC and EC accesses the flash over eSPI.

1. Requires eSPI interface to be up and initialized by both SOC and EC.
2. On G3 exit, EC de-asserts RSMRST# (GPIO055 TBD), initializes eSPI, reads its image from SPINOR over eSPI, loads into its internal SRAM and notifies PCD-H. This is handled by the ROM in EC chip before giving control to the downloaded FW image.
3. The downloaded flash image continues the power sequencing until SOC is out of reset and BIOS starts executing.

4. This flash sharing mechanism also allows access during runtime which is handled by the downloaded EC FW image.
5. Soft strap in descriptor to restrict EC to access EC FW region only.
6. EC image Offset 1000H.

Below is the high-level block diagram for MAF Flash sharing.

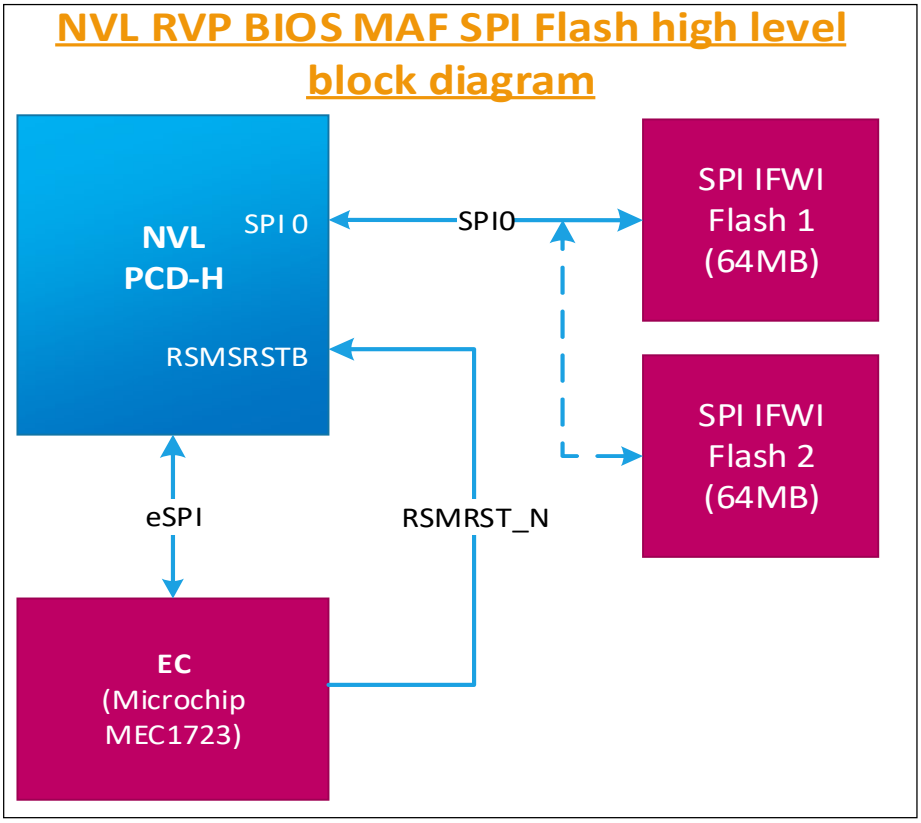


Figure 19-3: MAF high level block diagram

19.6.3. Slave Attached Flash Sharing (SAF)

SAF is one of the Flash sharing Mechanism where EC is the master which access flash over its SPI Controller and PCD-H sharing the same flash will access over eSPI. MEC1723 Microchip Embedded Controller can support SAF mode flashing. Rework is required on RVP to support SAF.

NVL SOC is allocated dedicated regions (for each of the supported masters) within the eSPI slave-attached flash devices. SOC has read, write, and erase access to these regions, as well as any other regions that maybe permitted by the region protections set in the Flash Descriptor. The Slave will optionally perform additional checking on SOC provided address. In case of an error due to incorrect address or any other issues it will synthesize an unsuccessful completion back to the eSPI Master.

The SAF supports Flash Read, Write and Erase operations. It also supports the RPMC, Read SFDP and Read JEDEC ID commands.

In this topology, the SPI flash is connected to EC and SOC accesses the flash over eSPI.

1. On G3 exit, EC loads its entire image into its internal SRAM, verifies the image (if supported as root of trust), and then de-asserts RSMRST# for PCD-H/SOC to access flash over eSPI.
2. EC must meet the timing requirements for the SAF to avoid FW access latencies to avoid any impact to responsiveness or boot time.

3. EC should enable the access to regions based on soft straps in the descriptor.

Below is the high-level block diagram for SAF Flash sharing:

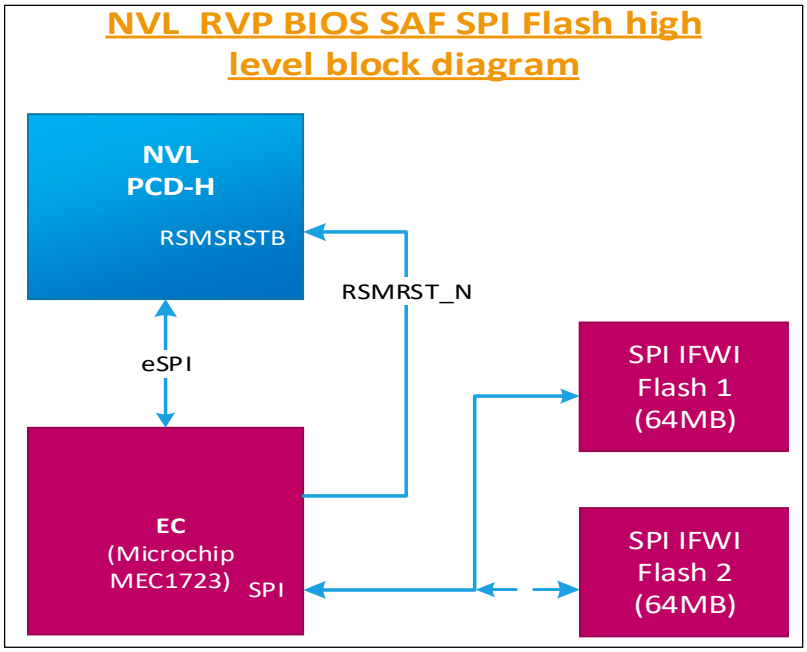


Figure 19-4: SAF high level block diagram

19.7. PCH-IOE Flash

NVL RVP supports a dedicated SPI Flash for PCH.IOE There will not be flash sharing between PCD and PCH.
For PCH.IOE a single flash with capacity of 8MB is supported at 100MHz Frequency. SPI flash for PCH.IOE will be 1.8V and without RPMC support.
There is no FW resiliency support from NVMe SSD for this flash for PCH-IOE FW.
There will be a dedicated TPM Header/Dediprog Programming Header for this flash.
To access PCH IOE Flash remotely, paddle board and cable needs to be used from the existing TTK3 as shown in Figure 19-1.

19.8. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

20. Security

20.1. Overview

Trusted Platform Module (TPM) is a Trusted Computing Group (TCG) low-cost security solution to increase confidence on system security. The TPM is a device that resides on the motherboard and is connected to SOC/PCH using Serial Peripheral Interface (SPI) bus to communicate with the rest of the platform.

The objective of the TPM is to establish a baseline of platform integrity and enhance system security. TPM's are available from several integrated circuit vendors in the form of a silicon component and accompanying software. When integrated into the PC, a TPM provides protected storage of platform data allowing for platform-level authentication toward the goal of making data files, transactions, and communication more trustworthy.

The NVL RVP supports only SPI based TPM AIC. It doesn't support eSPI based TPM as no such device exists. LPC based TPM as LPC interface is no longer supported.

20.2. Security domain platform MRD/PRD

Below is the platform MRD/ PRD for the Security domain.

- Platform MRD HSD link.
- Security Domain platform PRD HSD link.

20.3. Security domain RVP LZ/ PRD

TBD

Below table capture the security domain feature set on NVL RVPs.

Table 90: Security Domain Feature set

Si#	Security domain features	NVL-AX/AM
1	**SPI based TPM**	Yes
2	**TPM support**	Yes

20.4. HW BOM

Below table capture the HW BOM for security domain supported on NVL RVPs.

Table 91: NVL AX/AM Security Domain HW BOM

Si#	HW BOM Description	Part#/ IPN	Vendor	HSD link
1	SPI based TPM Module	1. SLB967x 2. NPCT75x / NPCT76x 3. ST33KTPM2x 4. Z32H330TC-SPIDCARD-751	1. Infineon 2. Nuvoton 3. ST Micro 4. Nations Tech	TBD

20.5. AIC List

Below table capture the AIC list for security domain supported on NVL RVPs.

Table 92: NVL AX/AM Security domain AIC List

Si#	HW BOM Description	Part#/ IPN	Vendor	HSD link
1	SPI TPM AIC	TBD	Intel	TBD

20.6. SPI based TPM

The NVL RVP supports the discrete SPI TPM AIC over the primary SPI0 interface that connects the SOC/PCD-H and the BIOS flash memory.

The SPI based TPM AIC should be plugged into the traditional 20pin BIOS flash header. The IPN of the 2x10 header is G25403-002 with pin definition given in below table.

Table 93: Pinout Details for SPI based TPM

Signal Name	Pin No	Pin No	Signal Name
KEYING	1	2	CHIP_SELECT_ 0
RSMRST	3	4	CHIP_SELECT_ 1
GND	5	6	+3.3A OR +1.8A
SPI_CLK	7	8	DQ2
DQ3	9	10	SPI_MISO
HOLD	11	12	SPI_MOSI
CHIP_SELECT_ 2	13	14	GND
WRITE_PROTECT	15	16	TP_SERIAL_IRQ
SPI_TPM_INT_N	17	18	+3.3A OR +1.8A
PLTRST	19	20	RSVD

SPI TPM AIC hosts the SLB9672Vx chip from Infineon. It supports an SPI interface with a transfer rate of up to 43MHz. Its power management is handled internally; no explicit power-down or standby mode is required. The device automatically enters a low-power state after each successful command/response transaction. If a transaction is started on the SPI bus from the host platform, the device will wake immediately and will return to the low-power mode after the transaction has been finished.

20.7. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

21. Power Delivery & Sequencing

21.1. Overview

In this section, all the NVL Ax RVP power delivery implementation details (with respect to energy management, rest of the platform power delivery, IMVP9.3 VR, power sequencing, voltage margining, power accumulator and PnP requirement) are covered.

High level SoC Power scheme of NVL Ax RVP is shown in figure below.

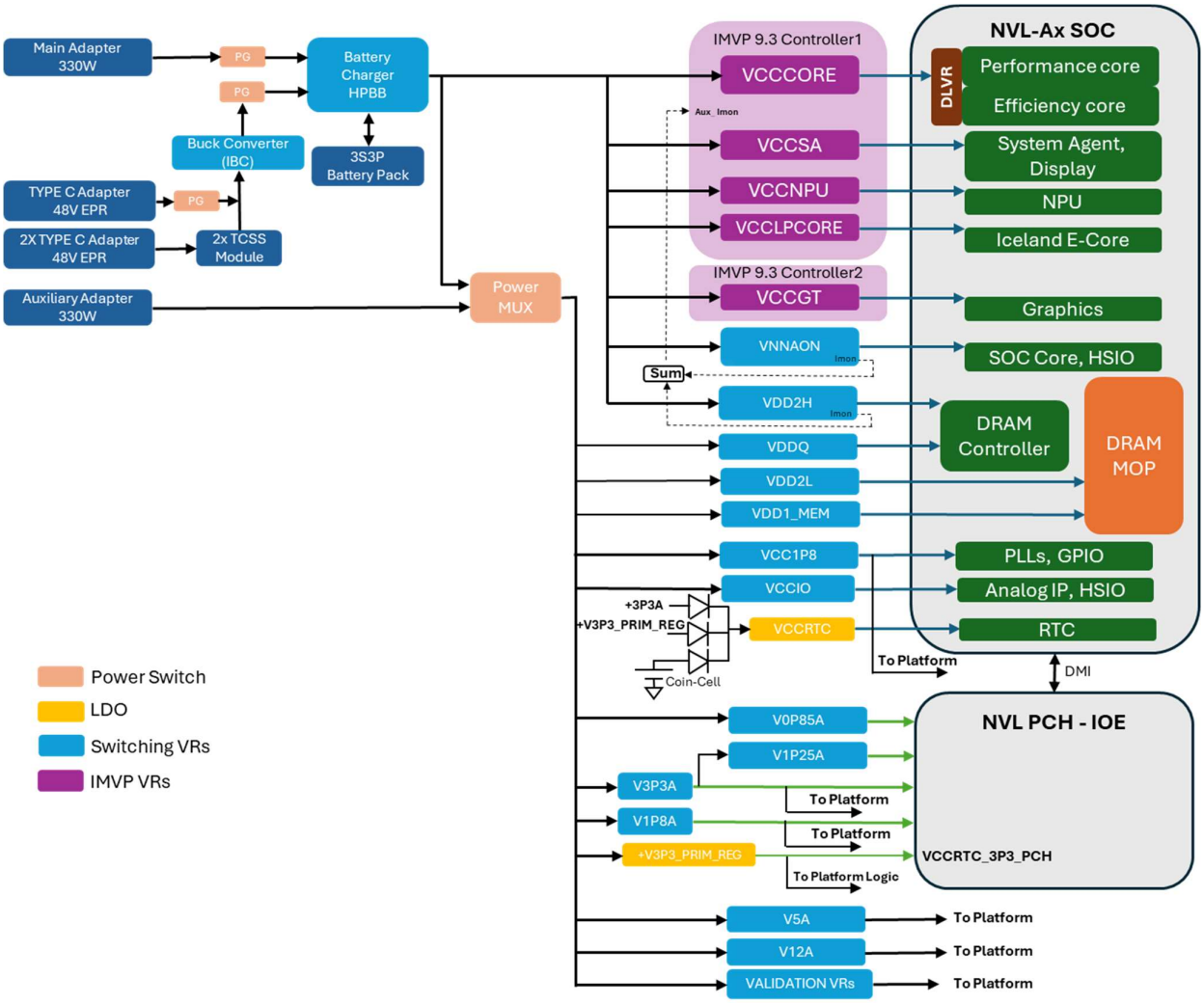


Figure 21-1: NVL-Ax High Level SoC Power Scheme

21.2. Platform PRD/MRD

NVL Ax Platform MRD details are provided in the LINK

NVL Ax Platform PRD details are provided in the LINK

21.3. NVL Ax RVP PD PRD

NVL Ax RVP Power delivery list of RVP PRD's are provided in the LINK

21.4. NVL Ax RVP LZ PD Details

NVL Ax RVP Landing zone details about power delivery are mentioned below table.

Table 94: NVL Ax Power delivery Landing zone

Sl.No	Domain Feature	Support
1	ATX 12V Aux power supply support - multi rail	No TBD
2	DC barrel Jack (Primary AC brick Support)	Yes
3	DC barrel Jack (Aux AC brick Support)	Yes
4	Type-C Power Delivery w/ EPR@ 48V	2x No's - EPR 48V PD via TCSS Module 1X Onboard EPR Type C PD
5	RTC Battery Holder	Yes
6	Discrete IMVP VR controller	Motherboard solder down
8	PMIC support for memory PD	No
9	Load switches/ Validation - debug VRs	Yes
12	Battery charger support	Yes
13	Battery support	3S battery
14	Connected standby mode	Yes
15	DeepSx mode	No
16	Pseudo G3 support (AC & DC)	Yes
17	Wake sources	Wake event link
18	Force PS_ON jumper	NA – No ATX support

21.5. NVL Ax RVP PD HW BOM

NVL Ax RVP PD Hardware BoM details mentioned in the table below. (TBD)

Table 95: NVL AX RVP PD HW BoM

Sl.No	HW BOM Description	Part#/ IPN	Vendor
1	IMVP9.3 controller1: VCCCORE+VCCNPU+VCCSA+VCC_LPCORE	AOZ71049QI (TBD)	AOZ (TBD)
2	IMVP9.3 controller2: VCCGT	AOZ71049QI (TBD)	AOZ (TBD)
3	Battery charger controller Hybrid Power Boost (HPB)	ISL95522AHRZ	Renesas
4	TC EPR Intermediate Bus converter (IBC) 48V/28V to 20V (3 Level Buck Converter)	RAA489300A3GNP	Renesas
5	Main Adapter	M85984-001	FSP TECHNOLOGY INC.
6	Aux adapter	M85984-001/ J82210-001	FSP TECHNOLOGY INC. / LITEON TECHNOLOGY CORP

7	Battery pack 3S, 8760.0MAH	K71137-001	
8	Power sequencer	SLG7NT48284V	Renesas
9	+V5A & +V3P3A	TPS51285A	TI
10	+V12A	ISL81401AFRZ	Renesas
11	+V1P8A	RT6220AGQUF	Richtek
12	+VNNAON (with Aux Imon capability)	AOZ23567BQI	Alpha & Omega semi
13	+VCCIO	TPS51375L	TI
15	+VDD1	TPS51375L	TI
16	+VDD2H (with Aux Imon capability)	AOZ23567BQI	Alpha & Omega semi
17	+VDD2L	TPS51375L	TI
18	+VDDQ	NB792GD-Z	MPS
19	+VCC1P2_RTC	TPS7A0312DQNR	TI
20	+V0.85A_PCH	TPS51219RTER	TI
21	+V1.05A _PCH	TPS62826DMQR	TI
22	+V1P8A_PCH	TPS62826DMQR	TI

21.6. Power Sources

NVL can be powered through single/dual 330W standard AC adapter, a Type C Adapter and/or a Battery pack. To support PL4 power number of NVL silicon's without battery, use auxiliary AC adapter along with 330W main AC adapter.

Recommendation: For NVL-AX, 330W adapter is mandatory for all the validation except Performance, use Type C adapter or battery pack on need basis. For performance validation in absence of battery pack use dual AC adapter.

21.6.1. Standard AC adapter

Standard main AC adapter alone cannot support NVL PL4 power number. Along with the main AC adapter either battery pack or aux AC adapter is required to support NVL PL4 performance power number.

330W AC adapter IPN : M85984-001

Description: AC/DC ADAPTER, 100V-240V Input, 50-60HZ, 19.5V/16.9A Output

21.6.2. Type C Adapter

There are three USB-C ports with PD supported on NVL AX/AM RVP. The Type C ports on TCSS module support and on board Type port support EPR voltages up to 48V.

NVL Ax RVP doesn't support for Type C PD PDO profile less than 28V (TBD).

Note: For dead battery boot with a type-c adapter, min profile requirement is 180W (TBD).

21.6.3. Battery Pack

A 3S3P battery pack is being selected for NVL RVP with maximum capacity of 99Whr.

3S3P battery pack **IPN:** K71137-001

21.6.4. Auxiliary Adapter

An auxiliary adapter is required for supporting PL4 current number along with the main AC adapter in the absence of battery pack while performing performance related validation. Auxiliary AC adapter powers all the rails (ROP) except IMVP rails.

Platform will not boot with auxiliary adapter alone. When using an auxiliary AC adapter, it is recommended to plug in the main AC adapter first and then followed by an auxiliary AC adapter.

Note: Auxiliary AC adapter can be used either 330W AC adapter or 240W AC adapter based on availability.

Auxiliary AC adapter IPN: M85984-001(330W AC adapter)/ IPN: J82210-001(230W AC adapter).

Table 96: Power Sources & Priority on NVL RVPs

Available Sources	Priority Given To
Standard main AC Adapter + Type C Adapter	Standard main AC Adapter
SPR Type-C Adapter + EPR Type-C Adapter	EPR Type-C Adapter
EPR1 Type-C Adapter + EPR2 Type-C Adapter	Whichever is having higher power output

Note: Smooth/seamless transition from Type-C adapter to AC adapter and vice versa is not supported if battery is not connected.

21.7. Key Power Delivery Subsystems

The platform power delivery has three key sub-systems which are Energy management, Rest of the platform (RoP) power delivery and CPU power Delivery (including IMVP9.3 VR).

21.7.1. Energy Management Sub-System

Battery charger and USB power delivery comes under the energy management sub-system. A Buck HPB charger is used to charge the battery pack. System powered up from either main AC adapter or Type-C adapter and battery packs supplement the power based on system power demand.

21.7.2. Rest of the Platform Power Delivery

RoP power delivery sub-system includes discrete voltage regulators (non-SVID), power sequencing and load switches. Discrete VR's powering the CPU (non-SVID), PCH and platform components.

21.7.3. IMVP9.3 Sub-system

NVL Ax CPU requires five different SVID rails (VCCCORE, VCCGT, VCCNPU VCCSA and VCC_LPECORE). Two IMVP9.3 compliant controllers are used for generating these rails. All IMVP rails Vboot voltage is 0V and the IMVP VR's output voltages change based on workloads via SVID communication

IMVP VR phase count requirement is given in below table.

Table 97: IMVP VR Phase Count

NVL-Ax **IMVP Controller1: VCCCORE+VCCNPU+VCCSA+VCC_LPCORE** **IMVP Controller2: VCCGT**
1. IMVP VR Controller Phase count: 6+2+1+1 2. IMVP VR Controller Phase count: 6+0+0+0 For VCCCORE and VCCGT – 4 PWM signals will drive 6 phase DRMOS. PWM1, PWM2 will drive single DRMOS, PWM3 and PWM4 will drive two DRMOS each.

Icc max, TDC and load line targets for NVL Ax processor is shown in the table below.

Table 98: Processor Line Power Specifications (TBD)

Rail Name	NVL-AX 8+16+4 512EU (125W CTDP)				NVL-Am 4+8+4 256EU (60W CTDP)			
	Icc_max.raw / Iccmax.app	I_PL2 / I_TDC	Icc_max.trip	DC/AC Load line	Icc_max.raw/ Iccmax.app	I_PL2/ I_TDC	Icc_max.trip	DC/AC Load line
VCCCORE (FVM)	202 A / 141 A	88 A	160 A	2.0 mΩ	146 A / 102 A	60 A / 56 A	116 A	2.0 mΩ
VCCGT (FVM)	315 A / 132 A	77 A	150 A	0 / 1.5 mΩ	160 A / 105 A	63 A / 59 A	120 A	0 / 1.5 mΩ
VCCNPU (FVM)	80 A / 70 A	35 A	80 A	3.5 mΩ	80 A / 70 A	35 A	80 A	3.5 mΩ
VCCSA (FVM)	55 A / 35 A	20 A	40 A	5.0 mΩ	55 A / 35 A	20 A	40 A	5.0 mΩ
VCC_LPECORE (NO FVM)	35 A	16 A	N/A	6.0 mΩ	35A	18 A	N/A	6.0 mΩ

Note: RVP design will cater to IMVP rails for Ax and Am processor by providing necessary PDBOM placeholders and design changes based on PI team input

21.8. Critical Rails and Default Voltage Levels

The below table for all the critical rails and the default regulated voltages.

Table 99: Critical Voltage Rails with default regulated voltage

Voltage Regulator	Typical Voltage	Comments
+VCCCORE	0V (Boot Voltage) 0V-1.52V	CPU adjusts the output voltage through SVID.
+VCCGT	0V (Boot Voltage) 0V-1.52V	CPU adjusts the output voltage through SVID.
+VCCNPU	0V (Boot Voltage) 0V-1.52V	CPU adjusts the output voltage through SVID.
+VCCSA	0V (Boot Voltage) 0V-1.52V	CPU adjusts the output voltage through SVID.
+ VCC_LPECORE	0V (Boot Voltage) 0V-1.52V	CPU adjusts the output voltage through SVID.
+VNNAON	0.77V	CPU rail, Need to provide Iout info to AuxImon
+VDD2H	1.07V (LP5x MOP)?	Shared rail (LP5x memory + CPU), Need to provide Iout info to AuxImon
+VDDQ	0.52/0.32V (LP5x MOP)	Shared rail (LP5x memory + CPU)
+VDD2L	0.92V	LP5x Memory (For DVFSC support)
+VDD1	1.8V (LP5x MOP)	LP5x Memory
+VCCIO	1.25V	CPU rail
+V3.3A	3.3V	PCH IOE + Platform
+V5A	5.0V	Platform
+V1.8A	1.8V	CPU + Platform
+V0.85A	0.85V	PCH IOE rail
+V1.05A	1.05V	PCH IOE rail
+VRTC	1.2V	CPU
+V12A	12V	PCIE slot

21.9. Power Map for NVL Ax RVP

NVL Power map would be placed in LINK which includes platform components.

NVL RVP Power delivery details with respect to SoC, PCH-IOE shown in figure below.

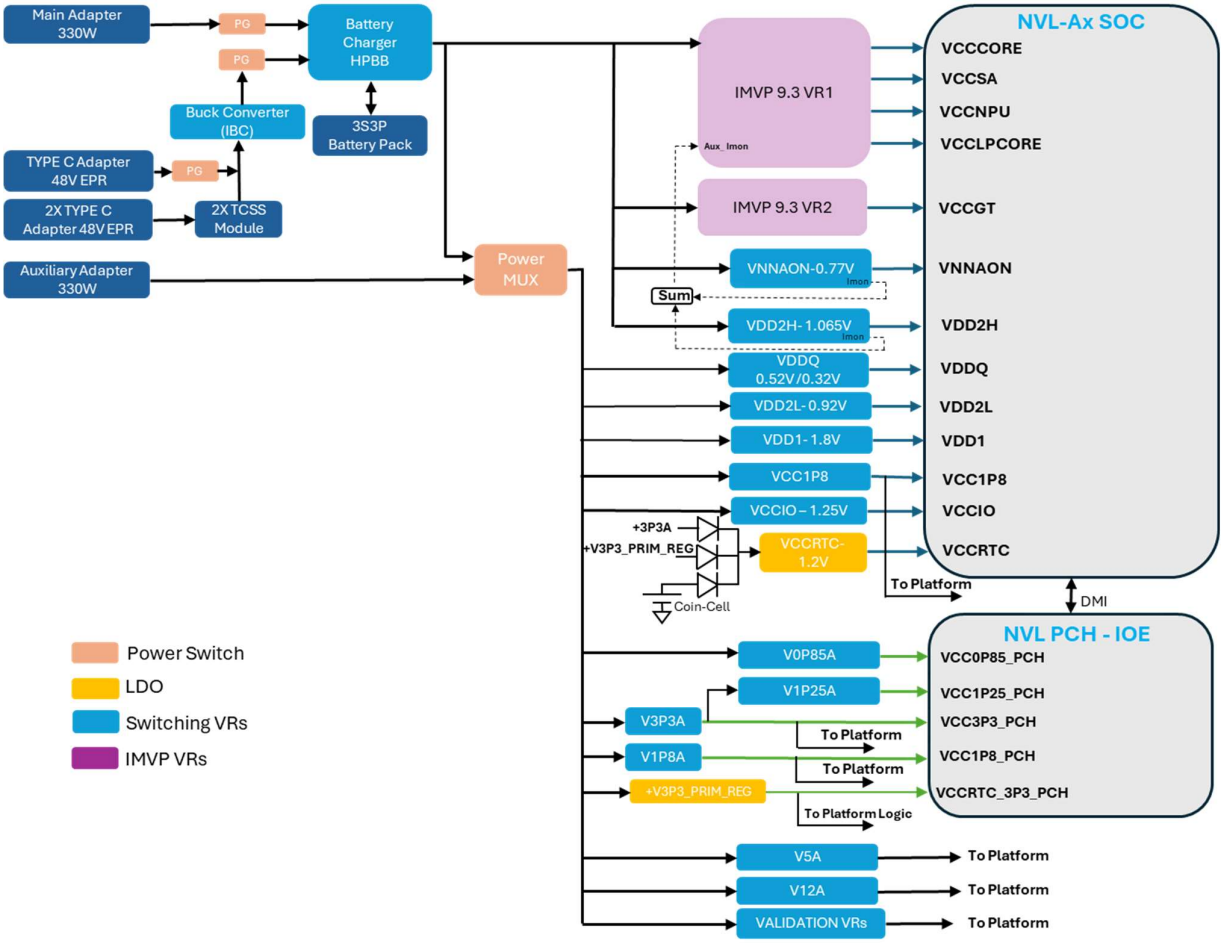


Figure 21-2: NVL Ax RVP Power Delivery Block diagram

21.10. Power Sequencing

- RSMRST_N signal indicates all primary rails are stable
- IMVP9.3 voltage regulators are enabled by ALL_SYS_PWRGD signal which indicates all the platform rails are stable.
- PCH_PWROK signal indicates all CPU IMVP VRs are stable
- VCCCORE, VCCGT, VCCNPU, VCCSA and VCC_LPECORE IMVP9.3 VRs have Zero boot voltage requirements.
- SVID communication is required to change the voltage of IMVP9.3 VRs.
- NVL Ax RVP supports Pseudo G3 state in both **AC Adapter mode & battery pack mode.**
- NVL Ax RVP supports the RTC rail timing requirements in dead coin cell scenario.
- **NVL Ax RVP sequence is same with or without PCH**.

NVL RVP Power sequencing diagram is available at LINK

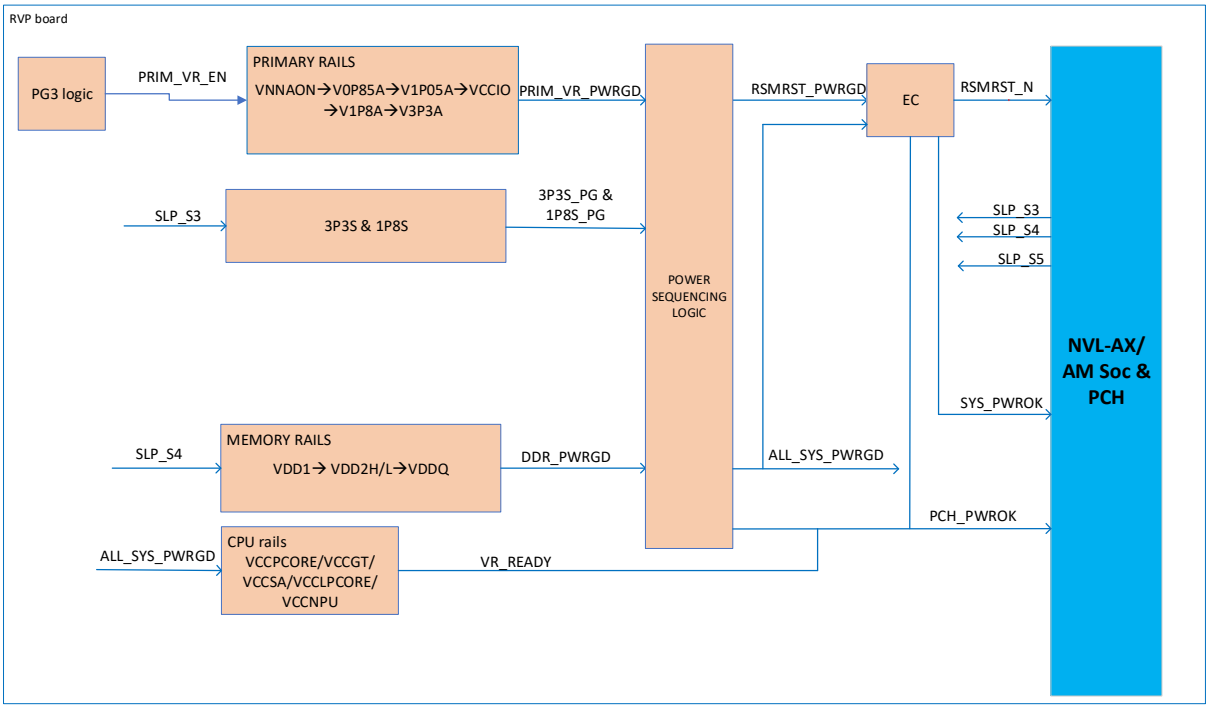


Figure 21-3: NVL Ax RVP Power Sequence Block diagram

22. GPIOs

22.1. Overview

The SOC General Purpose Input/output (GPIO) signals are grouped into multiple groups (such as GPP_A, GPP_B, and so on) and are powered by the SOC/PCD-H Primary well. Many GPIO signals are multiplexed with other native functions.

The high-level features of GPIO:

- Support 1.8V GPIO only
- GPIO Serial Expansion (GSX) bus mux on existing GPIO pins
- All GP Input are capable of generating an IRQ interrupt based on software configured level or edge-triggered event
- All GP Input are capable of generating SCI
- All GP Input are capable of generating wake event
- Selective GP Input are capable of generating NMI or SMI#
- GPIO supports glitch free during power sequencing, and when switching mode of operation (see GPIO spreadsheet for pins with exception)
- Supports software configured GP Input polarity
- Supports GPIO mode input sensing (Rx) disable
- Support RCOMP for GPIO pins (LP)

Below table captures NVL RVP GPIO Power group mapping.

Table 100: GPIO Power group mapping (Subjected to change based on the converged Pin list)

Si#	Power Group	Number of pins
1	GPP_A	17
2	GPP_B	25
3	GPP_C	21
4	GPP_D	21
5	GPP_E	22
6	GPP_F	20
7	GPP_H	21
8	GPP_S	8
9	GPP_V	18

NVL AX/AM GPIO mapping document for RVP SKU shall be captured in sharepoint (TBD).

All the SOC/PCH GPIO pins will be routed though resistor which will help in debugging.

22.2. RCOMPs

RCOMP's in NVL platform are listed below.

The RCOMP details will be updated for the next release of HAS.

Table 101: RCOMP Resistor Values (TBD)

Si#	Pin Name	Integrated vs Onboard	Description	Termination
1	**DDI_RCOMP**	Integrated	eDP PHY RCOMP, analog connection point for an external bias resistor to ground	200 ohms 1%
2	**SOC_REFRCOMP_ISCLK**		Connected to an external precision resistor for XCLK bias voltage generation	180 ohms 1%
3	**TYPEC_RCOMP**			200 ohms 1%
4	**PCIE4A_RCOMP**	Onboard (POC)	analog connection point for an external bias resistor to ground	200 ohms 1%
5	**PCIE4B_RCOMP**	Onboard (POC)	analog connection point for an external bias resistor to ground	200 ohms 1%
6	**USB3_RCOMP**	Onboard (POC)	USB3 MPHY RCOMP, analog connection point for an external bias resistor to ground	200 ohms 1%
7	**CSI_RCOMP**	Onboard	CSI DPHY RCOMP, analog connection point for an external bias resistor to ground	200 ohms 1%
8	**USB2A_RCOMP**		USB Resistor Bias, analog connection points for an external resistor to ground.	200 ohms 1%
9	**USB2B_RCOMP**			200 ohms 1%
10	**CNV_RCOMP**	Onboard	WiFi DPHY RCOMP, analog connection point for an external bias resistor to ground	200 ohms 1%
11	**SNDW_RCOMP**	Onboard	SoundWire buffer RCOMP, analog connection point for an external bias resistor to ground	200 ohms 1%
12	**UFS_RCOMP**	Onboard (POC)	UFS MPHY RCOMP, analog connection point for an external bias resistor to ground	200 ohms 1%
13	**DDR_RCOMP**			100 ohms 1%
14	**PCIE5_RCOMP**	Integrated		200 ohms 1%
15	**PCIE5A_RCOMP**	Integrated		200 ohms 1%

23. On board Hardware Straps

23.1. Overview

The NVL RVP takes care of the default hardware strap configuration for both CPU and PCH to ensure normal functionality. NVL RVP will provide on-board Pull-up/Pull-down resistor stuffing options for each strap. The strap configuration options along with default setting is given in below tables. Please refer to pin mapping for more info.

Reference:

PCD-H Pin list:

https://docs.intel.com/documents/pch_doc/NVL/PCD-H/HAS/Chap03_NVL_Pins/nvl-pcd-h_pinlist.html

NVL PCH Pin list:
https://docs.intel.com/documents/pch_doc/NVL/PCH/HAS/Chap03_NVL_PCH_Pins_Chap18_GPIO_Automation/Chap03_NVL_PCH_Pins_Chap18_GPIO_Automation.html

23.2. NVL PCD-H Hardware strap

Below table captures hardware strap for NVL PCD-H SOC based on pin list version 34. Final strap setting will be updated in HAS rev 1.0.

Table 102: hardware strap for NVL PCD-H SOC

GPIO #	When Sampled	Termination	HVM Strap	Pin Strap Usage	Output Signal	Polarity
xxgpp_d_12	PCH_PWROK	20K PD	No	No Reboot	gpcom_strap_no_reboot	No reboot if sampled high
xxgpp_b_14	PCH_PWROK	20K PD	No	Top swap override	gpcom_strap_top_swap_override	Top Swap is enabled if sampled high
xxgpp_b_23	RSMRSTB	20K PD	No	“RTC” PLL (POR) or XTAL	gpcom_strap_rtcdist_is_xtal	Default RTC PLL distribution source 1 = 38.4MHz XTAL (Survivability usage only) 0 = “RTC” PLL @76.8MHz. This is the POR, and the default. *This pin strap is for survivability usage only and expected to be further qualified with the “Personality Strap’ aka “A0 only Strap” outside of GPIO prior to being used by iSClk.
xxgpp_c_8	RSMRSTB	20K PD	No	TLS Confidentiality Enable	gpcom_strap_tls_cfen	TLS conf enabled if sampled high
xxgpp_c_5	RSMRSTB	20K PD	No	eSPI Disabled (previously called "EC-less Platform")	gpcom_strap_espi_disable	ESPI is disabled if sampled high
xxgpp_c_15	RSMRSTB	20K PD	No	XTAL Input Mode**[0]**	gpcom_strap_xtal_in_mode0	XTAL input mode 0: XTAL attached - **default** 1: Single-ended crystal

						input HVM/BI testing to pull-up this strap to select Single-Ended
xxgpp_v_17	PCH_PWROK	20K PD	No	Flash descriptor security override (commonly referred as FDO strap)	gpcom_strap_flashdesc_security_override	Security measures defined in the Flash Descriptor is overriden if sampled high
xxgpp_e_6	RSMRSTB	20K PU	No	JTAG ODT Disable	gpcom_strap_jtag_odt_disable_b	JTAG ODT is disabled if sampled low
xxgpp_e_9	RSMRSTB	None	**Yes**	RTCPLL Pre Divider Enable (HVM use only)	gpcom_strap_rtcpll_prediv_en	RTCPLL Pre Divider Enable 0 – Bypass pre-divider (functional; 32.768KHz input) 1 – Enable /125 pre-divider (HVM; 4MHz input) *This strap is qualified by DFXTESTMODE
xxgpp_e_10	RSMRSTB	None	**Yes**	XTAL Input Frequency *HVM/BI mode only	gpcom_strap_xtal_sedivsel	Single-ended reference clock divider select 0 – Divider Bypass (functional) - **default** 1 – Divide by 4 (100MHz HVM mode) *This strap is qualified by DFXTESTMODE
xxgpp_f_2	RSMRSTB	20K PU	No	M.2 CNV modes / Integrated CNV Enable/Disable	gpcom_strap_intg_cnv_disable	M.2 CNV modes 0 = Integrated CNV enable 1 = Integrated CNV disable
xxgpp_f_19	RSMRSTB	20K PD	No	Skip RTC Clock Stabilization Delay (IOTG Boot Time Reduction)	gpcom_strap_rtc_stblz_delay_bypass	Skip RTC Clock Stabilization Delay (IOTG Boot Time Reduction) 0 = No bypass (default) 1= Bypass/Skip 95ms RTC clock stabilization delay
xxgpp_h_0	RSMRSTB	20K PD	No	eSPI Flash Sharing Mode	gpcom_strap_espi_share_mode	Master attached flash sharing (MAFS) if sampled low, else slave attached flash sharing (SAFS)
xxgpp_h_1	RSMRSTB	20K PD	No	Enable/Disable SPI Flash Descriptor Recovery	gpcom_strap_nist_en	Flash Descriptor Recovery for NIST SP800-193 0 - Flash descriptor recovery disable - **default** 1 - Flash descriptor recovery enables
xxgpp_h_2	RSMRSTB	20K PD	No	SPI Flash Descriptor Recovery Source -	gpcom_strap_nist_src	Flash Descriptor Recovery Source for NIST SP800-193 0 - Flash descriptor

				Internal/External		recovery internal source - **default** 1 - Flash descriptor recovery external source
xxspi0_io_2	RSMRSTB	20K PU	No	Consent Strap	gpcom_strap_consent_b	Consent strap is enabled if sampled low
xxspi0_io_3	RSMRSTB	20K PU	No	Personality Strap (A0 only, disabled by RevID)	gpcom_strap_personality_b	Personality strap is enabled if sampled low
xxdbg_pmode	RSMRSTB	20K PU	No	DFXTESTMODE active	gpcom_strap_dfxtestmode_active_b	Assert DFXTESTMODE to enable other straps to take effect if sampled low
xxjtagx	RSMRSTB	20K PD	No	JTAGX ODT selection	gpcom_strap_jtagx	JTAGX ODT selection 0 - JTAGX ODT enable =1 1 - JTAGX ODT enable = JTAG ODT Disable STRAP
xxgpp_d_3	RSMRSTB	20K PD	No	PCH.IOE Mode Enable. Used by PMC, SPBC, PXP, PMA, CSE, ESE	gpcom_strap_pch_ioe_mode_en	'0' (default): PCH.IOE Mode is disabled '1': PCH.IOE Mode is enabled

23.3. NVL PCH IOE Hardware strap

Below table captures hardware strap for NVL PCH based on pin list version 37. Final strap setting will be updated in HAS rev 1.0.

Table 103: hardware strap for NVL PCH

GPIO #	When sampled	Termination	HVM Strap	Pin Strap Usage	Output Signal	Polarity
GPP_R_2	PCH_PWROK	20K PD	No	Top swap override	gpcom_strap_top_swap_override	Top Swap is enabled if sampled high
GPP_B_3	PCH_PWROK	20K PD	No	Flash descriptor security override	gpcom_strap_flashdesc_security_override	Security measures defined in the Flash Descriptor is overriden if sampled high
GPP_I_9	PCH_PWROK	20K PD	No	No Reboot	gpcom_strap_no_reboot	No reboot if sampled high
GPP_C_2	RSMRSTB	20K PD	No	TLS Confidentiality Enable	gpcom_strap_tls_cfen	TLS conf enabled if sampled high
GPP_C_5	RSMRSTB	20K PD	No	eSPI Disabled (previously called "EC-less Platform")	gpcom_strap_espi_disable	ESPI is disabled if sampled high
SPI0_MOSI_IO_0	RSMRSTB	20K PD	No	Spare 2	gpcom_strap_spare_2	Security measures defined in the Flash Descriptor is overriden if sampled high
GPP_B_19	RSMRSTB	20K PD	No	PSTM Mode	gpcom_strap_pstm_mode	PSTM mode 1- PCH Standalone Testmode 0- Normal functional mode
SPI0_IO_2	RSMRSTB	None	No	Spare	gpcom_strap_spare	
SPI0_IO_3	RSMRSTB	None	No	Personality Strap (A0 only, disabled by RevID)	gpcom_strap_personality_b	Personality strap is enabled if sampled low

GPP_H_11	RSMRSTB	20K PD	No	eSPI Flash Sharing Mode	gpcom_strap_espi_share_mode	0: Master attached flash sharing (MAFS) 1: slave attached flash sharing (SAFS)
GPP_H_14	RSMRSTB	20K PD	No	JTAG ODT Disable	gpcom_strap_jtag_odt_disable_b	JTAG ODT is disabled if sampled low
GPP_H_17	RSMRSTB	20K PD	No	SPI VCCIO configuration	gpcom_strap_spi_v1p8mode	SPI VCCIO@1.8V if sampled high, else 3.3V
DBG_ PMODE	RSMRSTB	20K PU	No	DFXTESTMODE active	gpcom_strap_dfxtestmode_active_b	Assert DFXTESTMODE to enable other straps to take effect if sampled low
GPP_E_9	RSMRSTB	None	**Yes**	Ring Oscillator Bypass (HVM only)	gpcom_strap_ring_osc_bypass_hvm	Ring Oscillator Bypass 0 – Output is not bypassed 1 – Output is bypassed *This strap is qualified by DFXTESTMODE
GPP_E_10	RSMRSTB	None	**Yes**	RESERVED	gpcom_strap_xtal_in_freq0_hvm	Updated to RESERVED. NVPS ISCLK xtal_sedivcel_strap removal https://hsdes.intel.com/appstore/article/#/15015629847
GPP_E_11	RSMRSTB	None	**Yes**	RESERVED	gpcom_strap_xtal_in_freq1_hvm	Updated to RESERVED. NVPS ISCLK xtal_sedivcel_strap removal https://hsdes.intel.com/appstore/article/#/15015629847
GPP_I_16	RSMRSTB	20K PD	No	Client vs Server CPU (a.k.a JTAG CPU family voltage select)	gpcom_strap_jtag_cpu_v1p25mode	Client vs Server CPU (a.k.a. JTAG CPU family voltage select) 0- with Client CPU. JTAG is 1.25V 1- with Server CPU. JTAG is 1.0V
GPD_7	DSW_PWROK	None	No	XTAL Input Mode**[0]**	gpcom_strap_xtal_in_mode0	XTAL input mode 0: XTAL attached **- default** 1: Single-ended crystal input HVM/BI testing to pull-up this strap to select Single-Ended
GPD_12	**DSW_PWROK**	None	No	PCH.IOE GPIO Pad Mode Enable	gpcom_strap_ioe_gpio_padmode_enable	PCH.IOE GPIO pad mode select enabled if sample high
GPP_J_1	RSMRSTB	20K PD	No	XTAL FREQ SEL0	gpcom_strap_xtal_freq_sel0	XTAL frequency selection 0 – 38.4MHz (default) 1 – 25MHz
GPP_J_3	RSMRSTB	20K PU	No	M.2 CNV modes / Integrated CNV Enable/Disable	gpcom_strap_intg_cnv_disable	M.2 CNV modes 0 – Integrated CNV enable 1 – Integrated CNV disable

GPP_I_13	PCH_PWROK	20K PD	No	Boot BIOS Strap (BBS)	gpcom_strap_bbs	BIOS fetches are routed based on this strap. 0 – BIOS fetches are routed to SPI (MAF) or the eSPI Flash Channel (SAF). 1 – BIOS fetches are routed to the eSPI Peripheral Channel.
JTAGX	RSMRSTB	20K PD	No	JTAGX ODT selection	gpcom_strap_jtagx	JTAGX ODT selection 0 - JTAGX ODT enable =1 1 - JTAGX ODT enable = JTAG ODT Disable STRAP
GPP_B_12	RSMRSTB	20K PD	No	Enable/Disable SPI Flash Descripto Recovery	gpcom_strap_nist_en	Flash Descripto Recovery for NIST SP800-193 0 - Flash descriptor recovery disable (default) 1- Flash descriptor recovery enable
GPP_H_0	RSMRSTB	20K PD	No	SPI Flash Descriptor Recovery Source - Internal/External	gpcom_strap_nist_src	Flash Descripto Recovery for NIST SP800-193 0 - Flash descriptor recovery internal source (default) 1- Flash descriptor recovery external source

24. PSS

24.1. Overview

PSS is Processor Secured Storage interface that is primarily intended for tracking platform specific information in a factory like environment. The PSS interface enables platform specific information to be stored on the On-board memory (EEPROM) and access the stored information by either I2C or RFID reader. The information can be uploaded to a Central Database which will then be accessible by internal labs for the purpose of tracking and proactively reviewing current hardware and software status. Information like reworks implemented on the specific platform can be stored in the PSS EEPROM chip.

PSS interface design is a standard implementation on all Intel RVP boards and NVL RVP shall follow the same circuit and design as its predecessors.

The PSS chip should be able to be read by an external reader at a distance greater than 1 meter from the Platform that contains the PSS chip in an open environment.

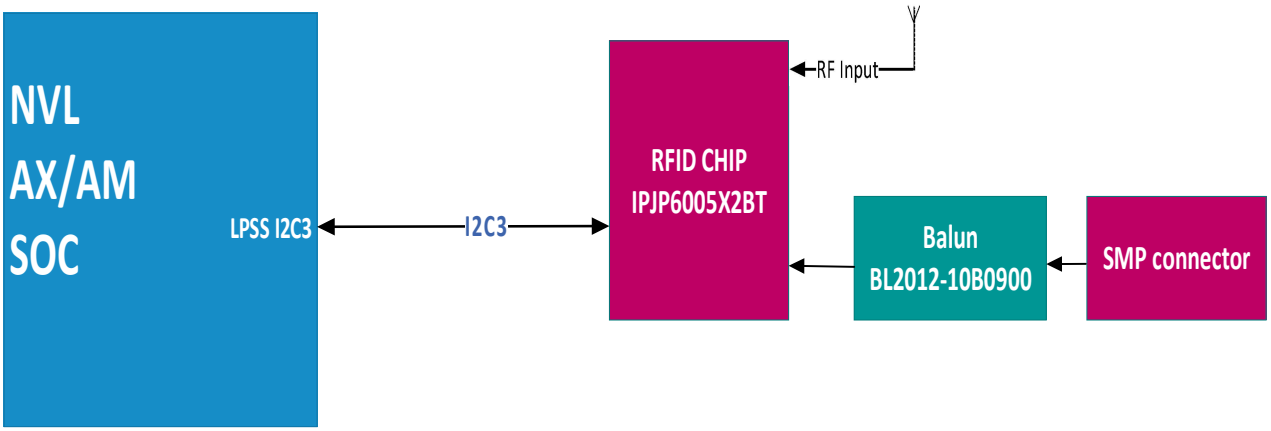


Figure 24-1 :PSS Circuit high level block diagram for NVL AX/AM

The NVL RVP supports 8K memory size RFID chip with options for I2C connection from SOC.

The RVP supports both on board PCB slot edge antenna as well as the external Antenna options. The external antenna path will have the on board BL2012 series Balun chip from ACX. The PSS shall have the properties mentioned in the table below.

Table 104: PSS Properties on NVL

Si#	Description	Value
1	**Memory Size**	8kbit
2	**Memory Configuration**	12 x 128 NVM / OTP
3	**I2C Interface**	Device Driver-OS
4	**Reader Communication**	Gen2 RFID Commands

25. PPV (Processor/Product Platform Validation)

25.1. Overview

NVL AX/AM RVP is used in PPV environment for silicon screening.

25.2. PPV support on NVL AX/AM RVP

NVL AX/AM RVP shall support the necessary mechanical and PPV specific socket KOZs required for PPV environment without deviating from POR platform requirements. IO Assignment is covered in the respective IO section. That should be referred to know the exact mapping.

PPV SKUs will support below HDRs and connectors for key board level interface requirements:

1. Side band header – for key control signals. All customization which was done for PPV will be removed from PM side band header since PPV is not using PM side band header anymore (TTK3 and SINAI are used currently)
    a. Pins 35/37/39 go to the FRU ROM after the "isolation" jumpers, **will be removed**
    b. +VRTC_BATT the RTC Coin Cell battery connection to the PM side band HDR **will be removed**
    c. There are 4 EDM pins, connect to DUT as appropriate: for U Package for example, 2 to CPU, 1 to EDRAM, with stuffing option for second PCH if applicable, and one to primary PCH.
    d. Pins 4/6 are the SMBUS connected to the Port80 PLD
2. InTEC header – for thermal connection
3. SINAI2 header – for analog voltage and current sense and a couple DIOs
4. TTK3 Header- for BIOS emulation on SPI signals, via SAC2 AIC
5. Debug log capability using either DB9 connector or via uUSB
6. PDBOM implementation will be same as RVP and there is no separate PD BOM for PPV.
7. Header for I2C CLK/DATA connecting to on board FRU EEPROM.
8. PCIe x1 slot – One PCI-E x1 slot on the board to cable PCI-E to host system to connect other PCIe devices down-stream from a bridge.
9. PPV Board ID should retain the same as RVP Board ID. BOM ID will be changed 0x5

PPV SKUs will have the support for below custom BRD requirements:

1. CPU pad must have Solder Resist Opening (SRO) 25um radius / 50um diameter larger than the pad, example 250um pad would need 300um SRO. This is to optimize socket alignment.
2. No silk-screen under socket zero height KOZ area, to avoid silk screen lifting socket slightly off board, impacting socket reliability.
3. NiAu plating (aka ENIG) with Nickel and Gold on surface for the PPV specific builds PCB to make more durable for use in factory.
4. Must review DFx (DFM/DFT) with SIMS team to enable smooth transfer of PPV builds to SIMS to support future builds past PRQ.

25.3. PPV Specific RVP LZ/ PRD

- RVP Delta PRD link.

26. Debug and Validation Hooks

26.1. Overview

A system could be debugged either via one of the following methods:

- Open Chassis debug – this includes XDP, MIPI60 (LTB) with two MIPI60 headers on NVL AX/AM RVP.
- Closed chassis debug – USB debug (USB2/USB3/OOB).

This section of RVP HAS shall cover the overview of SoC debug architecture followed by debug interfaces of SoC that are supported in the RVP. It shall also list down various SoC validation hooks and cover all the validation interfaces that are supported in this NVL RVP for users to debug the Silicon.

26.2. Debug domain platform MRD/PRDs

Below is the platform MRD/ PRD for the Debug domain.

- Platform MRD HSD link.

26.3. Debug domain RVP LZ/ PRD

TBD

Below table capture the debug feature support on NVL AX/AM RVP.

Table 105: Debug feature support on NVL AX/AM RVP

Si#	Debug domain features	RVP
1	**MIPI60 Debug Connector for SoC**	Yes
2	**MIPI60 Debug Connector for PCH.IOE**	Yes
3	**VISA probing via THC (Touch panel) header 1**	Yes
4	**VISA probing via THC (Touch panel) header 2**	Yes
5	**I3C Debug from SoC (over Type C con)**	Zbb'd
6	**USB2 DbC (over Type C USB2 con)**	Yes
7	**USB2 DbC (over Type-A USB2 con)**	Yes
8	**USB3 DbC (over Type C USB3 con)**	Yes
9	**USB3 DbC (over Type-A USB3 con)**	TBD
10	**OOB 2 wire (over Type C)**	NA - Not POR for NVL
11	**CMC**	No
12	**SMP connector for silicon View pins**	Yes
13	**SINAI2 / NEVO Connector**	Yes
14	**Bit blaster**	TBD
15	**INTEC Connector**	Yes
16	**SVID probing header (3x1)**	Yes
17	**SVID Jumper**	NA - Not POR from LNL onwards
18	**FIVR debug header for SoC/ CPU**	Yes
19	**FIVR debug header for PCH**	NA

20	**RVP DAC support**	Yes, Refer HAS for more details
21	**UCP-SQUID**	Yes, Refer HAS for more details
22	**RVP NEST**	Yes, Refer HAS for more details
23	**Port 80 Display on board**	Yes
24	**LED's: - (CAPSLOCK, NUMLOCK, PWRBTN, S0, S3, S4, S5, SUS, ME, PM, CATERR, WLAN, BT, WWAN, CHGR, HGR, CS, C10, PCIE_LINK_DOWN)**	Yes, refer HAS for latest LED list
25	**DEBUG - SERIAL PORT uAB USB CONNECTOR**	Yes
26	**Debug - SERIAL UART HDR (1x4)**	Yes
27	**DEBUG - SERIAL PORT DB9 CONNECTOR**	NA - Not POR
28	**PM Side band header**	Yes
29	**Power validation/ sequence header**	Yes
30	**PROCESSOR FAN CONTROL PWM and TACHO**	Yes
31	**PROCESSOR FAN (Always on fan header)**	Yes
32	**RTC/SRTC Reset HDR's**	Yes
33	**Power measurement Resistors (PMR) supports**	Yes
34	**POWER MEASUREMENT HEADER**	Yes
35	**POWER MEASUREMENT ID DETECTION HDR**	Yes
36	**POWER MEASUREMENT SPARE HDR**	Yes
37	**MECC AIC (EC AIC) connector**	No
38	**PS2 keyboard header (1x5)**	Yes
39	**PS2 mouse header (1x5)**	NA - Not POR from PTL onwards
40	**Scan matrix keyboard connector**	Yes
41	**Scan matrix keyboard backlight control connector (1x6)**	Yes
42	**SAS KBC/ CTRL header (2x8)**	Yes
43	**SAS PORT 80 header (2x8)**	Yes
44	**SAS front panel (2x8) header**	Yes
45	**SAS SLP header (2x4)**	Yes

26.4. AIC List

Below is the table for Debug AIC list supported on NVL RVP.

Table 106: NVL Debug AIC List

Si#	Add In Card (AIC) Description	IPN	Rev #	Wiki link
1	**SINAI/NEVO AIC**	(TBD)	(TBD)	Link
2	**TTK3 AIC**	(TBD)	(TBD)	Link

26.5. SoC Debug architecture - Introduction

NVL SoC Architecture overview here.

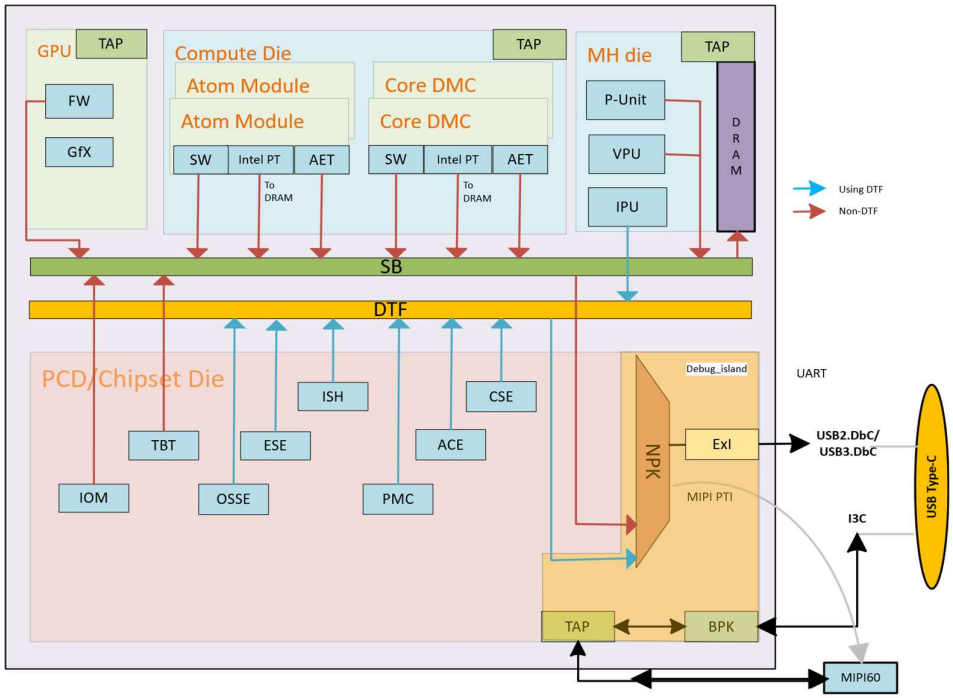


Figure 26-1: NVL without PCH-IOE Debug Architectural Overview

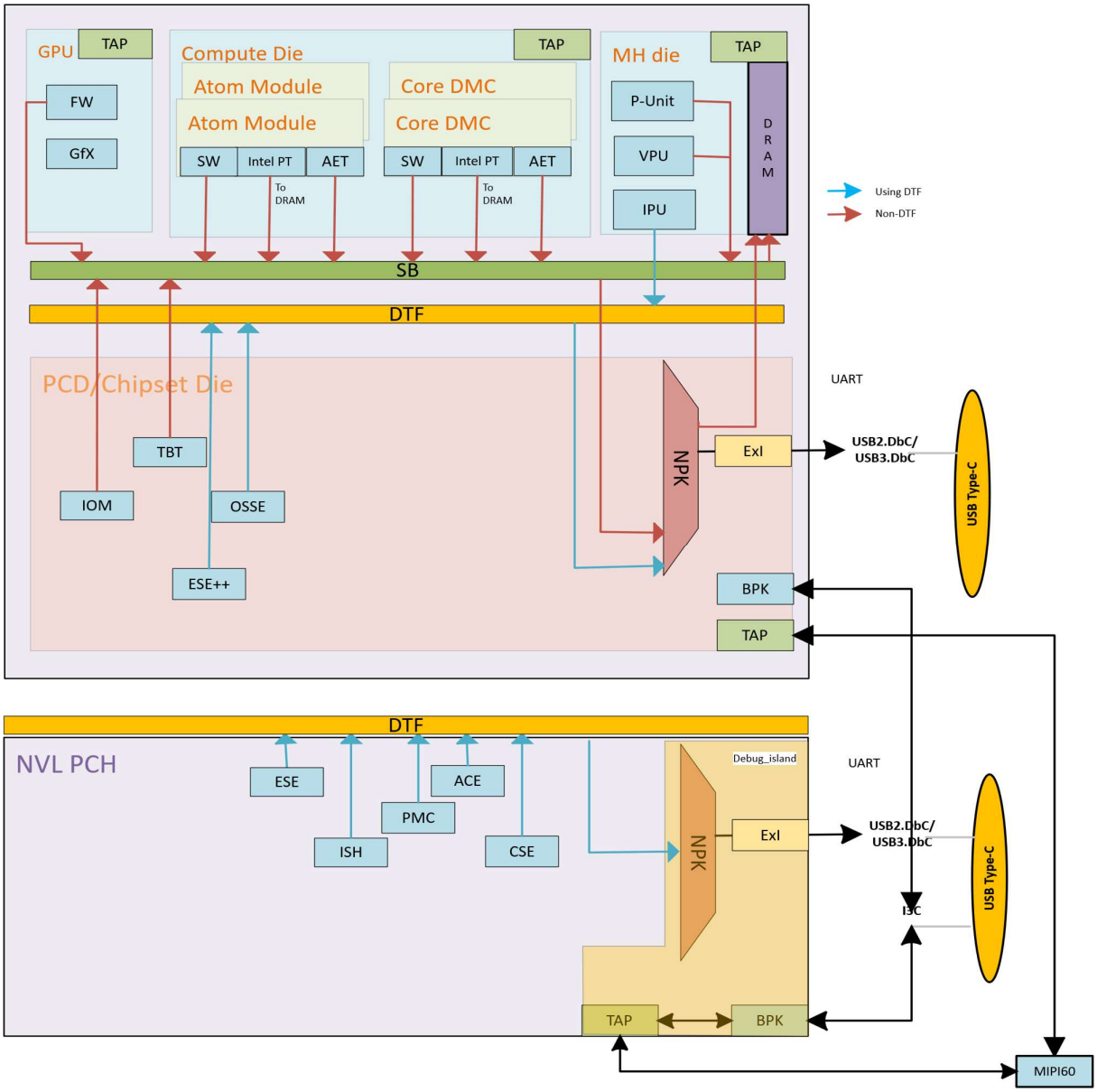


Figure 26-2: NVL with PCH-IOE Debug Architectural Overview

Note:

1. NVL has GPU Die, Compute Dies and MH Die. The VPU has been moved to the MH Die.
2. The PCD/Chipset Die consists of NorthPeak (NPK) debug island and supports multiple debug interfaces like the USB/MIPI60/JTAG etc.
3. Debug Trace Fabric (DTF) and SB are the buses to carry traces to NorthPeak (NPK).
4. NVL PCH consists of NorthPeak (NPK) debug island and supports multiple debug interfaces. Debug Trace Fabric (DTF) is considered bus to carry traces to NorthPeak (NPK).

26.6. Boot flow debug

Boot flow debug is one of the most important debug scenarios to support. In general, boot flow referring to the period where power is supplied to the system, until first instruction fetches from CPU. Specifically, for NVL PCD, this period referring to RSMRST# de-asserted until PLTRST# de-asserted.

For NVL platform, boot flow is divided into 3 boot phases: Boot phase1 (Early boot phase), Boot phase2, and Boot Phase3. Boot phase1 is also call early boot phase. Refer to figure below for general boot flow.

To support boot flow debug, debug interface needs to be available to connect early enough in boot flow and has ability to temporary stop the boot flow for unlock and debug.

There are a few intercept points that a debug interface can halt the boot flow. There are "Platform Boot Stall", "CSE Boot Stall", "C-Die Boot Stall", and IA main core reset break.

Below is the Debug Boot flow for NVL.

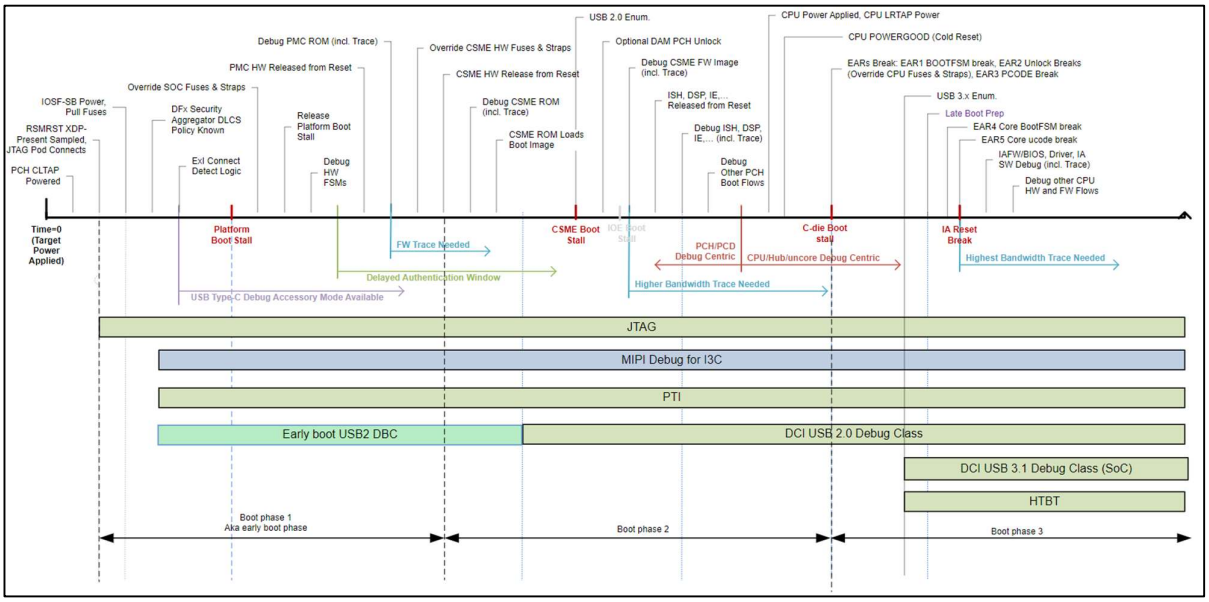


Figure 26-3: NVL boot flow debug

Early boot phase is the earliest a debug interface may intercept NVL PCD in boot flow. This is known as platform boot stall. A few debug interfaces are required to support boot flow during early boot phase. There is external MIPI60 Debug Port connector and early boot USB2 DBC.

"CSE Boot Stall" is the next point where debug interface can intercept. As the name suggested, CSE Boot Stall happen when CSE is booting. However, per definition, CSE boot stall does not happen right from the beginning of CSE ROM starts, but instead, CSE Boot Stall happen during CSE RBE execution. Only USB2 DbC supports CSE Boot Stall. Note that MIPI60 doesn't supports CSE Boot Stall.

"C-Die Boot Stall" are the same as previous client platform with CPU-PCH architecture.

After "C-Die Boot Stall", PMC will continue the boot flow to bring up Host IP and Compute die. The "C-Die Boot Stall" is equal to dielet boots tall or BootFSM break.

Following table show the debug interface and its earliest connection time w.r.t. boot flow.

Table 107: Boot Flow Debug vs. Debug Interface

Support	MIPI60 connector	USB2 DbC	USB3 DbC
Platform Boot stall	Yes	Yes	No
CSE Boot stall	No	Yes	No
CPU Boot stall	Yes	Yes	No
IA main core reset break	Yes	Yes	No

26.7. Debug interfaces supported by SoC

Following are the Debug interfaces supported by SoC

Table 108: NVL RVP Debug Support

Type	Interface Name	Supported in NVL RVP
Open Chassis	JTAG (over MIPI60)	Yes
	MIPI-PTI (over MIPI60)	Yes
Closed Chassis	USB2 DbC (over Type C)	Yes
	USB2 DbC (over USB2 port)	Yes
	*OOB 2 wire (over Type C)	No*
	I3C Debug (over Type C)	Z'bbd
	USB3 DbC (over Type C/Std-A)	Yes (Type-A & Type-C)

26.7.1. SMP Mapping of Validation Hooks

Validation signals on single SMP connector List is captured below. (TBD)

Only one signal at a time can be connected to SMP connector after resistor stuffing rework.

Table 109: Validation Hooks on SMP

SMP - 1	SMP - 2

SMP - 3	SMP - 4

SMP - 5	SMP - 6

SMP - 7	SMP - 8

SMP - 9	SMP - 10

SMP - 11	-
	-

26.8. Generic RVP debug features

26.8.1. Open Chassis Debug

Debug used for interfaces that are not placed inside a closed system is referred to as Open Chassis Debug. Types of Open Chassis:

- MIPI PTI
- JTAG

The MIPI PTI & JTAG signals are over the MIPI 60 Connector.

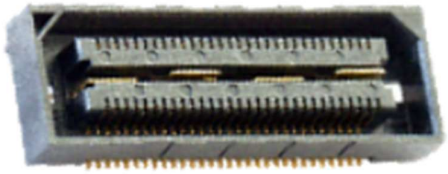


Figure 26-4: MIPI60 Debug Port (Samtec QSH-030-01 series)

The MIPI 60 Debug Port Interface enables communication between the Target System and Debug Tools. The MIPI 60 connector has power pins, JTAG, UART, I2C clock & data signals and different active low signals like POWER_BUTTON_N, CPU_EARLY_BREAK_N, PLATFORM_BOOT_STALL_N, Single RESET_N, RESET_BUTTON_N to initiate a target system cold boot, to stall the CPU boot sequence at the earliest CPU stall point to perform pre-boot configurations to Intel CPU's, to stall the platform boot sequence at the earliest stall point to perform pre-boot configurations to Intel PCH's and SoC's, to determine various Reset and Power states on the Target System, to initiate a Target System warm-reset without cycling power cycles respectively.

26.8.1.1. MIPI60 Debug Connector (TBD)

NVL AX/AM supports two configurations one with PCH-IOE and one without PCH-IOE.
Without PCH-IOE

- Single MIPI60 connector for PCD-H.

With PCH-IOE (TBD)

- Merged MIPI 60 connector for PCD-H and PCHS.
- Separate MIPI60 connectors for PCD-H.

NVL AX/AM PCD-H supports 4 channel VISA debug capability. Channel 3 & 4 VISA signals will be routed to MIPI 60 connector. Whereas Channel 1 & 2 VISA signals are muxed with Touch signals & will be routed to Touch connector.

NVL AX/AM PCH supports 2 channel VISA Debug capability. Channel 1 and 2 VISA will be routed to MIPI60 connector.

NVL AX/AM does not have NOA signals.

Below is the VISA Connector pinout:

Table 110: SoC VISA MIPI60 Connector Pinout (TBD)

MIPI60 Pin#	Intel DPS Generic Signal name	NVL Target Signal Name
3	TCK0	JTAG_PCD_TCK
51	TCK1	Res 0E pull-down to GND
9	TRST_N	JTAG_PCD_TRST_B
2	TMS	JTAG_PCD_TMS
5	TDI	JTAG_PCD_TDI
4	TDO	JTAG_PCD_TDO
10	PREQ_N	PREQ_B
11	PRDY_N	PRDY_B
8	TRST_PD	Defensive pull-down
42	HOOK[0] (CLTAP_PWRGOOD)	RSMRST_B
36	HOOK[3] (BOOT_HALT_N)	BOOTHALT_B
7	HOOK[6] (PMODE)	DBG_PMODE
38	HOOK[2] (EAR_N strap)	Test point
15	POD_PRESENT1_N (SOC)	SPI0_IO_2 (Strap)
17	POD_PRESENT2_N	Defensive pull-down
40	HOOK[1] (POWER_BTN_N)	Power_button_n
6	HOOK[7] / nReset (RESET_BTN_N)	Reset_button_n
34	RSVD[1]	No Connect
55	HOOK[8]	JTAG_PCD_MBPB_0
53	HOOK[9]	JTAG_PCD_MBPB_1
13	PTI_0_CLK	GPP_B_19
19..33 odd	PTI_0_DATA[0..7]	GPP_B_[2:8,18]
59	PTI_3_CLK	GPP_D_8
35..49 odd	PTI_0_DATA[8..15]/	GPP_B_[17,20,21,23]
14	PTI_1_CLK	GND
18..32 even	PTI_1_DATA[0..7]	No Connect
60	PTI_2_CLK	GND
44,46	RSVD[2..3]	No Connect
52	RSVD4	+V3P3A_VAL
54	DBG_UART_TX	UART1_TXD
56	DBG_UART_RX	UART1_RXD
48	I2C_SCL	SMB_CLK_S4
50	I2C_SDA	SMB_DATA_S4
1	VREF_DEBUG	+VCCIO_TERM_V1P25
12	VREF_TRACE	V1P8A
16	GND	GND
57	GND	GND
58	GND	GND

Link to Intel Debug Port Specification (DPS): IDPS

26.8.2. NVL RVP VISA connections

NVL RVP VISA connections are captured in below diagram.

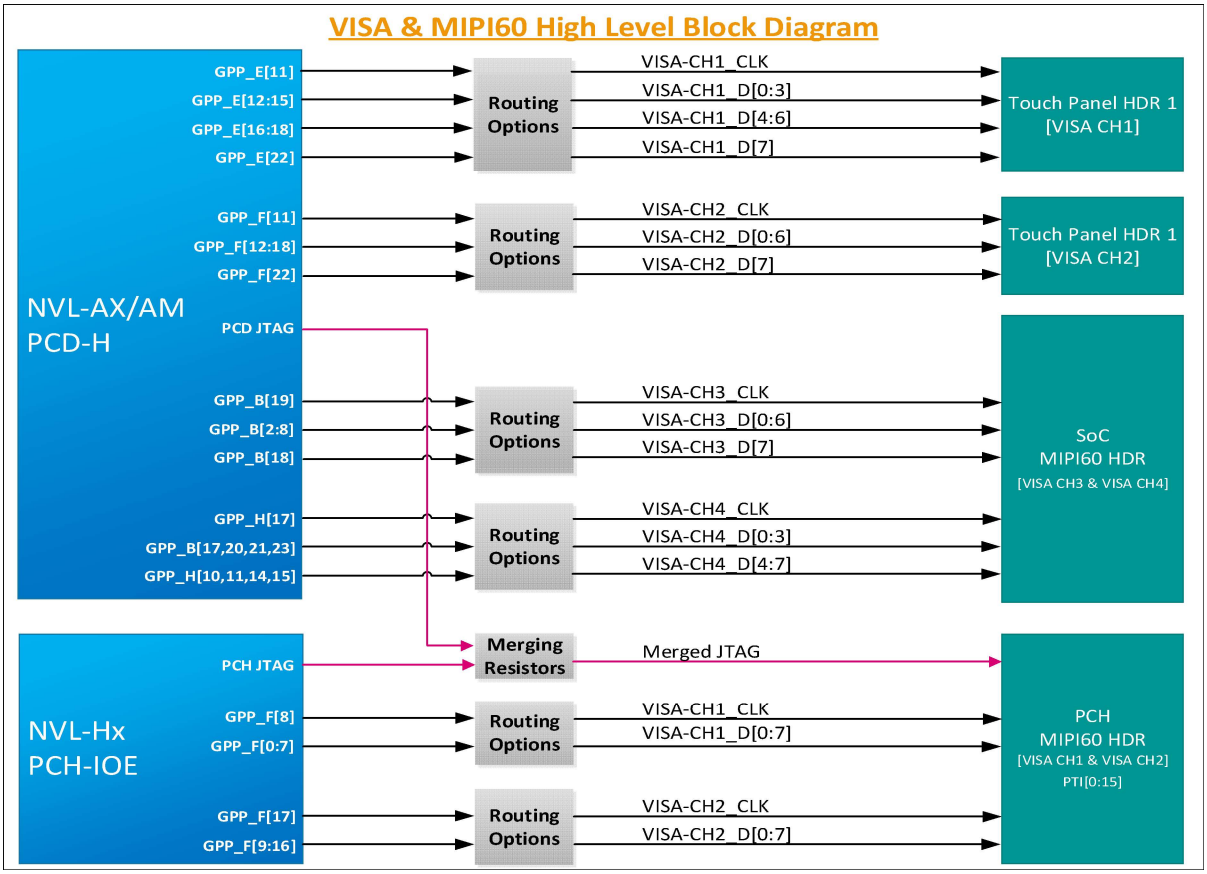


Figure 26-5: NVL AX/AM RVP VISA connections

26.8.3. Closed Chassis Debug

Debug using functional connections available in the complete, closed, form-factor system is referred to as Closed Chassis Debug.

Types of Closed Chassis:

1. Debug over USB 2.0
2. Debug over USB 3.0

26.8.3.1. Debug over USB 2.0

The Debug Class over USB 2.0 is supported on all USB 2.0 ports and uses the native USB protocol to transmit. USB2.0 debug class does require the use of the TS functional xHCI controller.

USB2 DBC Port 1 has enhanced capabilities beyond other USB2 ports and should be connected to an easily accessible USB Type-C port so these new features can be utilized. These features are enabled because USB2 DBC Port 1 is in “Debug Island”. The features include:

Able to connect very early in the boot sequence to support Connect First/Authorized Debug unlocks.

Able to remain connected and active during low power events (Sx and S0iX).

Connection does not affect device going to low power.

Since the Intel Trace Hub is also instantiated in Debug Island, traces can seamlessly transition overpower cycling events.

Supports all other traditional connection and debug capability.

For the Debug Class over USB 2.0 to operate, the TS must have debug enabled and the TS USB port used must be in the UFP role. The Type C is configured to UFP role when the PD controller detects Debug Accessory Mode. DTS is in the DFP role and TS is in the UFP role. The Std-A port must have the USB2 port manually configured to the UFP role in the FW straps using the mFIT tool and can't be used as functional port when it's configured for debug.

26.8.3.2. Debug over USB 3.0

The Debug Class over USB 3 is supported on all of the USB 3 ports from the PCH and CPU and uses the native USB protocol to transmit. USB 3 Debug Class does require the use of the functional controller. The Debug Class over USB 3 works over both Type A and Type C.

The Debug Class over USB 3 is only available during the S0 power state. Debug Class over USB 3.1 is first available after the platform reset de-assertion and when the CPU is running. The Debug Class over USB 3 does not survive through Sx power state transitions and across warm and cold resets. When the Debug Class over USB 3.1 is connected, the system will not be able to exit the S0 power state into lower states.

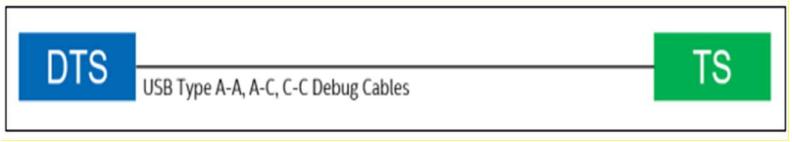


Figure 26-6: Illustrates the most basic connection between DTS and TS using just a USB Debug cable

26.8.3.3. Debug for I3C

I3C from SoC is Zbb'd in NVL Platform

26.8.4. Debug features supported in RVP

Below is the table for Debug features supported.

Table 111: Table depicting different debug interface supported in NVL

Debug Feature	Description	Details
SINAI2	SINAI2 is used for voltage & current sensing, current pump channels and GPIO manipulations.	SINAI2/NEVO
InTEC	InTEC is Integrated Thermal Environment Controller used for PECI and thermal monitoring of CPU thru the external InTEC AIC.	INTEC Header
PM sideband header	Most of the power sequencing related signals are terminated on this header, which can be used for debugging purpose. This header now being used by the RVP DAC AIC card which helps to enable remote debugging.	PM Sideband Header
Port80 Display Output	The NVL RVP supports the 4 digit 7-Segment LED display for Port80 debug messages	PORT80 Display Output
Serial Debug Console	Serial debug console over a micro-AB USB 2.0 receptacle port	Serial Debug Console
LED	LED indications for system states/status/errors.	LEDs
RVP Health DAC	A novel way to access remote hardware & accelerate debug	RVP Health DAC
UCP-SQUID	Low cost, Multi-Protocol and Remote programming solution	UCP-SQUID
RVP NEST	RVP NEST is a remote access farm hosted and maintained by RVP Team	RVP NEST
Box Stress Test	BST is an AIO integrated solution used for Voltage measurements, Voltage drive/margining, GPIO's manipulations, I2C master controller and Thermal Diodes measurements capabilities	Box Stress Tool

26.8.4.1. SINAI2/NEVO (Initial mapping, it is subjected to change. Will update it by HAS1.0)

SINAI2 is used for voltage & current sensing, current pump channels and GPIO manipulations. SINAI (believed to be the name of mountain where the Ten Commandments were given to Moses by God) is just an internal project name and does not have an acronym. The primary platform interface for SINAI2 is a 2x50, 100pin connector (IPN: D10221-001) for voltage margining and current sensing.

Sinai2 connectors has following types of pins:

1. GPIO: General purpose IOs. Can be configured as input or output and be configured as Open drain or CMOS.
2. GPIO-Fixed: IOs which should be routed to specific signals on the platform or stayed unconnected (if the feature is not needed). These have special topology which matches the relevant functionality.
3. DC3V3IO: General purpose IOs. Can be used to drive 3.3V signals. Good for stable signals (DC) like mux controls & straps. Currently only work as outputs.
4. ISNS [P/N]: Differential pair for sensing current through shunt resistors. Supports up to 160mV.
5. VSNS [P/N]: Differential pair for sensing voltage. Supports up to 3.2V in normal mode and 6.4V in extended mode.

6. IDRV: Current pumps output for voltage margining. Can drive/sink up to 14mA.
7. SPCL: Special purpose pins, which are used for power/GND or other maintenance functions in Sinai2. They must be connected as stated in the pin map.

SINAI2 special pins:

1. GND – should be connected to reference GND of the platform.
2. ~~VCCST – should be connected to VCCST plane~~
3. VCCIO – should be connected to VCCIO plane (normally 1.25V) for reference of MBP and all other GPIOs.
4. Setup done (pin 100 in sideband) – indicates that Sinai2 configuration is done and that the GPIOs are in programmed state. A good practice would be to connect this indication to the power sequence of the platform to prevent race between Sinai2 and other devices. Normally this signal is asserted ~900mS before CPU_POWERGOOD (if powered from the same power supply)

The actual utilization of the Vsense, Isense, Idrive & GPIO channels of Sinai2 is platform dependent. The pinout and channel allocation of SINAI2 interface will be finalized after reviewing the requirements from VFT representative. Multiple options would be supported using optional resistors. Resistor based stuff/unstuff option must be included in any GPIO and Isense path to Nevo connector.

26.8.4.1.1. Current Sensing Signals

Sinai2 senses current for measurement through the Sideband connector. Like in voltage sensing, the accuracy required from Sinai2 is very high. Moreover, in current sensing, Sinai2 is actually sensing low voltage levels (0-160mV) on a shunt resistor and errors and by routed traces will result in wrong current reading. Max bus voltage is 3.2V (common mode voltage). P/N traces to be taken from phase sense resistor (P/N) similar to PnP HDR routing.

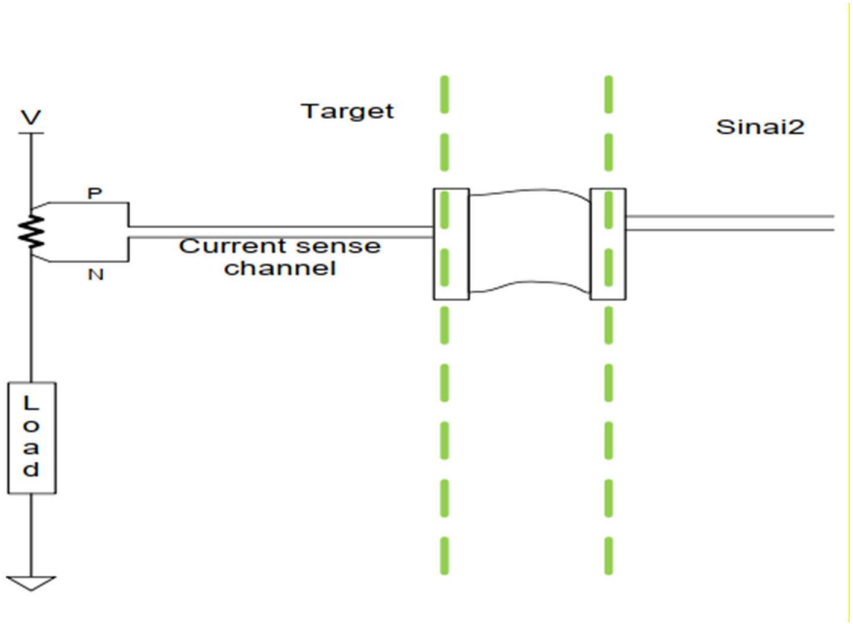


Figure 26-7: Current Sense Implementation

26.8.4.1.2. Sense resistor selection

It is important to note that the sense resistor selected for this circuitry should enable Sinai2 to measure the entire (or the desired) range of current to the load. For that, the voltage on that resistor in maximum current

condition should not exceed 160mV.A larger resistor will cause a cutoff in the range of sampling while a smaller resistor value will cause degradation of the granularity and accuracy of the sampling.

26.8.4.1.3. Routing Guidelines for Sense Signals

Sinai2 senses voltage rails for measurement through AVMC connector. The accuracy required from Sinai2 sensing is very high (less than 1mV), thus, the routing of the sense traces should get special attention. The Routing of AVMC sense signals will follow below guidelines:

1. The Voltage sense traces should be routed as differential pairs on the platform from the sensing point to the AVMC connector.
2. Voltage sense point should be tap from center of the PMR PAD
3. The traces differential impedance should be 80-100 Ω.
4. The traces should be routed in internal layers as far as possible from noisy parts (coils, oscillators, high frequency signals etc.)

26.8.4.1.4. SVID Signals to SINAI

SVID to SINAI2 connections is not part in any RVP SKUs of NVL since no team using SVID VR margining or validation over SINAI2 connector.

SVID VR margining will be done by using SVID BUS.

Below is the table for SINAI connector pinout.

Table 112: SINAI2 Connector pinout

Pin #	Pin Name (Option1 / Option2)	Type	Pin #	Pin Name (Option1 / Option2)	Type
1	**VSENSE_P<0>**	VSNSP	51	GPIO3	GPIO
2	**VSENSE_P<1>**	VSNSP	52	BCLKP	GPIO - FIXED
3	**VSENSE_N<0>**	VSNSN	53	GND	SPCL
4	**VSENSE_N<1>**	VSNSN	54	GND	SPCL
5	**VSENSE_P<2>**	VSNSP	55	ISense5N	ISNSN
6	**VSENSE_P<3>**	VSNSP	56	VSENSE_P<11> / I2C_Slave_SCL	VSNSP/GPIOFIXED
7	**VSENSE_N<2>**	VSNSN	57	ISense5P	ISNSP
8	**VSENSE_N<>**	VSNSN	58	VSENSE_N<11> / I2C_Slave_SDA	VSNSN/ GPIO - FIXED
9	**VSENSE_P<4>**	VSNSP	59	ISense6N	ISNSN
10	**VSENSE_P<5>**	VSNSP	60	VSENSE_P<12>	VSNSP
11	**VSENSE_N<4>**	VSNSN	61	ISense6P	ISNSP
12	**VSENSE_N<5>**	VSNSN	62	VSENSE_N<12>	VSNSN
13	**GPIO0**	GPIO	63	I2C_Master_SCL	GPIO - FIXED
14	**GPIO1**	GPIO	64	I2C_Master_SDA	GPIO - FIXED
15	**GND**	SPCL	65	GND	SPCL
16	**GND**	SPCL	66	GND	SPCL
17	**VSENSE_P<6> / SPI-MISO**	VSNSP/ GPIO - FIXED	67	ISense7N	ISNSN
18	**VSENSE_P<7> / SPI-MOSI**	VSNSP/ GPIO - FIXED	68	ISense8N	ISNSN

19	**VSENSE_N<6> / SPI-CLK**	VSNSN/ GPIO - FIXED	69	ISense7P	ISNSP
20	**VSENSE_N<7> / SPI-CS**	VSNSN/ GPIO - FIXED	70	ISense8P	ISNSP
21	**VSENSE_P<8>**	VSNSP	71	GPIO4	GPIO
22	**ISense0N**	ISNSN	72	GPIO5 / PECI_MUX_CTRL	GPIO - FIXED
23	**VSENSE_N<8>**	VSNSN	73	CPU_PWRGD	GPIO - FIXED
24	**ISense0P**	ISNSP	74	PLT_RESETN	GPIO - FIXED
25	**VSENSE_P<9>**	VSNSP	75	GPIO6	GPIO
26	**ISense1N**	ISNSN	76	PLT_RESTARTN	GPIO - FIXED
27	**VSENSE_N<9>**	VSNSN	77	GND	SPCL
28	**ISense1P**	ISNSP	78	GND	SPCL
29	**VSENSE_P<10> / PMSYNC**	VSNSP/ GPIO - FIXED	79	ISense9N	ISNSN
30	**CPU_SVID_OUT**	GPIO - FIXED	80	ISense10N	ISNSN
31	**VSENSE_N<10> / PECI_MON**	VSNSN/ GPIO - FIXED	81	ISense9P	ISNSP
32	**CPU_SVID_CLK**	GPIO - FIXED	82	ISense10P	ISNSP
33	**GND**	SPCL	83	PROCHOT(Drive)	GPIO - FIXED
34	**GND**	SPCL	84	VSENSE_P<13>	VSNSP
35	**CATERR**	GPIO - FIXED	85	VSENSE_N<13>	VSNSN
36	**CPU_SVID_ALRT**	GPIO - FIXED	86	VSENSE_P<14>	VSNSP
37	**PROCHOT**	GPIO - FIXED	87	VSENSE_N<14>	VSNSN
38	**THERMTRIP**	GPIO - FIXED	88	GPIO7	GPIO
39	**ISense2N**	ISNSN	89	VCCST	SPCL
40	**VRM_SVID_OUT**	GPIO - FIXED	90	VCCST	SPCL
41	**ISense2P**	ISNSP	91	GPIO8 / IDRIVE9	GPIO/IDRV
42	**VRM_SVID_CLK**	GPIO - FIXED	92	IDRIVE0	IDRV
43	**ISense3N**	ISNSN	93	IDRIVE1	IDRV
44	**GND**	SPCL	94	IDRIVE2	IDRV
45	**ISense3P**	ISNSP	95	IDRIVE3	IDRV
46	**VRM_SVID_ALRT**	GPIO - FIXED	96	IDRIVE4	IDRV
47	**ISense4N**	ISNSN	97	IDRIVE5	IDRV
48	**PECI**	GPIO - FIXED	98	IDRIVE6	IDRV
49	**ISense4P**	ISNSP	99	IDRIVE7	IDRV
50	**BCLKN**	GPIO - FIXED	100	IDRIVE8 / PLT_SETUP_DONE	IDRV/SPCL

26.8.4.2. INTEC Header

InTEC is Integrated Thermal Environment Controller used for PECI and thermal monitoring of CPU and PCH thru the external InTEC AIC. The platforms signals that enable the thermal control and monitoring are thermal DIODE signals and PECI signals from CPU and PCH. The platform connector part details are given in below table. Test points will be provided for PECI, FORCEPR# & THERMTRIP#, and CATERR# signals.

Table 113: INTEC Connector PN

Sl#	MFG	Mfg Part Number	IPN
1	Molex	501190-3027	G94240-001
2	Molex	501190-3017	G24701-002

The RVP supports G94240-001 part by default. The design details are given below. The link for pin mapping will be added later.

Below is the table for Platform design recommendations for Intec Signals:

Table 114: Platform Design Recommendations for InTEC signals

pin#	InTEC signal name	RVP Signal Connection	Comments
1	**THERMDA0_Sense**	VAL_THERMDA0_S	Thermal Diode 1
2	**THERMDC0_Sense**	VAL_THERMDC0_S	
3	**THERMDC0_Force**	VAL_THERMDC0_F	
4	**THERMDA0_Force**	VAL_THERMDA0_F	
5	**PROCHOT0**	PROCHOT_MON0_INTEC_N	PROCHOT Copy (LVTTL)
6	**GND**	GND	
7	**THERMDA1_Sense**	VAL_GCD_THERM_DA_S	GCD Die Thermal Diode 2
8	**THERMDC1_Sense**	VAL_GCD_THERM_DC_S	
9	**THERMDC1_Force**	VAL_GCD_THERM_DC_F	
10	**THERMDA1_Force**	VAL_GCD_THERM_DA_F	
11	**PROCHOT1_PECI Trigger**	NC	
12	**GND**	GND	
13	**THERMDA2_Sense**	VAL_SOC_THERM_DA_S	SOC Die Thermal Diode
14	**THERMDC2_Sense**	VAL_SOC_THERM_DC_S	
15	**THERMDC2_Force**	VAL_SOC_THERM_DC_F	
16	**THERMDA2_Force**	VAL_SOC_THERM_DA_F	
17	**PROCHOT2**	NC	
18	**GND**	GND	
19	**THERMDA3_Sense**	VAL_THERMDA1_S	Thermal Diode 2
20	**THERMDC3_Sense**	VAL_THERMDC1_S	
21	**THERMDC3_Force**	VAL_THERMDC1_F	
22	**THERMDA3_Force**	VAL_THERMDA1_F	
23	**PROCHOT3**	NC	
24	**GND**	GND	
25	**PECI0**	CPU_PECI	PECI Interface
26	**GND**	GND	
27	**VTT0**	+VCCIO_TERM_V1P25_INTEC	
28	**PECI0_Mux_Ctrl**	*PECI Mux Ctrl	
29	**PECI_Copy**	**PECI PROBING	
30	**GND**	GND	

26.8.4.2.1. PECI Signal

PECI is an Intel proprietary interface that provides a communication channel between Intel processors and external components such as Super IO (SIO) and Embedded Controllers (EC) to provide processor temperature, Turbo, Assured Power (cTDP), and Memory Throttling Control mechanisms and many other services. PECI is used for platform thermal management and real-time control and configuration of processor features and performance. PECI support eSPI is POR for NVL. Refer SINAI to CPU sideband optimization section for PECI implementation in NVL RVP.

26.8.4.3. PORT80 Display Output

The NVL RVP supports the 4 digit 7-Segment LED display for Port80 debug messages like all other previous generation RVPs. The Port80 LED driver will be SMBus based connected to the Embedded Controller (EC) on-board. The EC gets the port80 messages from PCD-H over the eSPI interface depending on the platform configuration.

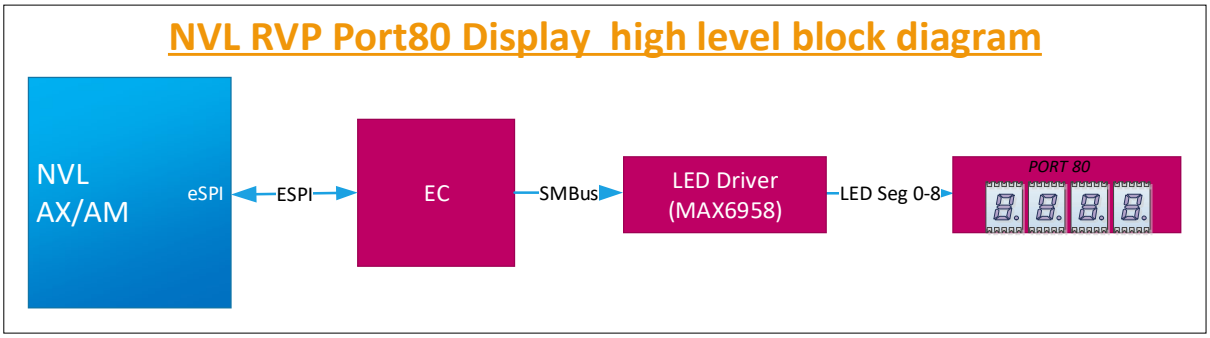


Figure 26-8: Port80 Functional Diagram

A 2x8 16-pin header 2.54mm pitch provided on the RVP design to bring the Port80 LED signals to front panel for validation purpose.

Below is the table for SAS Header and Pinout details.

Table 115: SAS Header

Sl#	MFG	Mfg. Part Number	IPN Number
1	WIESON TECHNOLOGIES CO., LTD	AC2100-0009-005-HH	K92628-001

Table 116: SAS Pinout

Signal Name	Pin #	Pin #	Signal Name
+V3P3A_R_VAL	1	2	LED_SEG8
GND	3	4	LED_SEG7
NO PIN	5	6	LED_SEG6
NC	7	8	LED_SEG5
NC	9	10	LED_SEG4
NC	11	12	LED_SEG3
RSVD_LED_SEG9	13	14	LED_SEG2
LED_SEG0	15	16	LED_SEG1

26.8.4.4. Serial Debug Console

The NVL RVP supports Serial debug console over a micro-AB USB 2.0 receptacle port. The RVP uses CP2105 Dual USB UART / FIFO IC for UART to USB2.0 conversion. The RVP will have option for EC and PCD-H connectivity for TX and RX signals while the CTS and RTS signals would be available from the PCD.H

Debug UART signals from EC shall be connected to mECC AIC connector and TTK3 connector as option in the design.

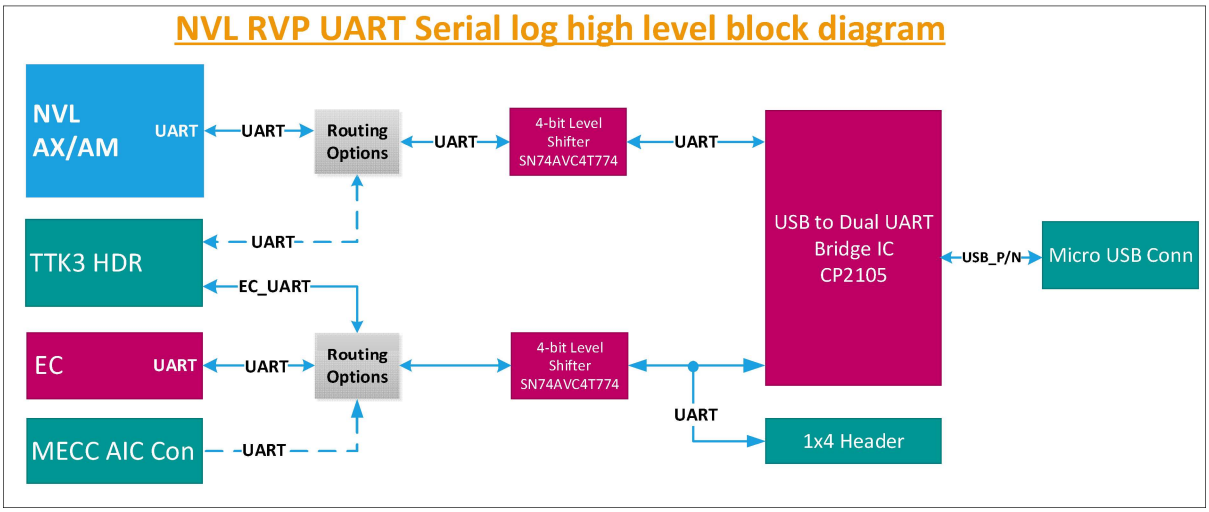


Figure 26-9: Serial debug console high level block diagram

Below is the table for Micro USB connector and pinout details:

Table 117: Micro USB connector

MFG	Mfg. Part Number	IPN Number
Hirose	ZX62RD-AB-5P8(30)	E10610-003

Table 118: Micro USB connector Pinout

Pin #	Signal Name
1	+V_VCC_USB_UART
2	USB_C_DEBUG_DM
3	USB_C_DEBUG_DP
4	NC
5	GND

26.8.4.5. LEDs

The NVL RVPs supports the following list of LEDs with their description given in below table

Table 119: RVP LEDs & Function

LED Name	Functional Description	LED Color
CAPSLOCK	Driven by EC to indicate the CAPSLOCK condition	GREEN
NUMLOCK	Driven by EC to indicate the NUMLOCK condition	GREEN
S0_LED_DRV	Indicates system entering state - S0	GREEN
S3_LED_DRV	Indicates system entering state – S3	GREEN
S4_LED_DRV	Indicates system entering state – S4	GREEN
S5_LED_DRV	Indicates system entering state – S5	GREEN
SUS_LED_DRV	Indicates system sleep state	GREEN
ME_LED_DRV	When asserted, INTEL ME is off	GREEN
CATERR	On board LED to indicate catastrophic event driven by CPU.	RED
M.2_WLAN_LED1	Indicates WLAN Module availability	GREEN
M.2_BT_LED2	Indicates BT Module availability	GREEN
PM_PWRBTN_LED	Driven by EC	GREEN
CHGR_LED_GATE_LED1	Driven By EC – Charging status	YELLOW
CHGR_LED_GATE_LED2	Driven By EC – Charging status	GREEN
CS_INDICATE_LED	Indicates whether system is in Connected Standby (CS)	GREEN
C10_GATE_LED	Indicated C10	GREEN
PCIE_LINK_DOWN	Indicates PCIe link down and will be routed to LED and to header	AMBER

Below is the table for Press buttons.

Table 120: NVL RVPs support following press buttons on board

Button	Function
Volume UP	Volume increase input to EC (Provided over header)
Volume DOWN	Volume decrease input to EC (Provided over header)
Power	External Power button input to the PCH and EC
Reset	External Reset button input to the PCH

Power and Reset signals will be routed to Front Panel Header and PM Side band header.

In general, for debug connectors, Refdes and pin numbering will be provided. Silkscreen for signal names can’t be supported. Also, default power on from G3 state (i.e., no need to press power button) will be supported.

26.9. Programming capabilities

Devices programmable in RVP

- BIOS SPI Flash
- EEPROMs
- PD AIC
- Retimer Flash
- TTK3
- EC Flash
- Dediprog

26.10. Details of debug tools

Below is the table for debug tools supported.

Table 121: Debug tools supported on NVL RVP

Debug support	Tool Description	Features
open chassis	Lauterbach Trace32 is used as the open chassis debug tool and connected via MIPI-60. The primary DTS is the CombiProbe v2 supporting merged JTAG and MIPI PTI.	1. Run-control 2. Trace extraction and analysis 3. Streaming trace via MIPI PTI (Intel Processor Trace) 4. CrashLog extraction and analysis 5. Custom Scripts (CScripts)
closed chassis	Intel System Studio is the main debug tool for closed-chassis debug over USB and for tracing.	1. Run-control 2. Trace extraction and analysis 3. CrashLog extraction and analysis 4. Custom Scripts (CScripts)

Source: Debug Link TBD

Below table shows a list of probes, associated cables, adapters dependencies. For more information refer to wiki link.

Table 122: List of probes, associated cables, adapters dependencies on NVL RVP

Sl#	Tool	Description	Wiki link
1	**XDP - Extensible Debug Port**	The XDP, also known as XDP3, XDP3b, XDP3br, Pod, ITP Blue Box is a JTAG debug adapter	XDP - Extensible Debug Port - Debug Tools Support - Intel Enterprise Wiki
2	**CCA - Closed Chassis Adapter**	CCA (Closed-Chassis Adapter) is one of the two ways of connecting the host and the target in the DCI (Direct Connect Interface) topology.	CCA - Closed Chassis Adapter - Debug Tools Support - Intel Enterprise Wiki
3	**DbC - Debug Cable**	DbC (Debug Cable) is one of the two ways of connecting the host and the target in the DCI (Direct Connect Interface) topology	DbC - Debug Cable - Debug Tools Support - Intel Enterprise Wiki
4	**LCP - Low-Cost Probe**	The LCP - Low-Cost Probe, is a probe manufactured by Lauterbach for Intel. It is similar in function to the Combi-Probe, but it has functional limitations built in which make it suitable for automation only, and not usable for regular debug.	LCP - Low Cost Probe - Debug Tools Support - Intel Enterprise Wiki
5	**LTB - Lauterbach Combiprobe**	The Combiprobe is a third-party developed JTAG probe built by Lauterbach (LTB) that can be used with Intel or Lauterbach's proprietary software; Trace32 and Powertrace.It connects to a MIPI60 JTAG connector or to a USB DCI connection via an adapter.	LTB - Lauterbach Combiprobe - Debug Tools Support - Intel Enterprise Wiki
6	**UTAG - USB JTAG Probe**	The UTAG4, is a JTAG debug adapter that works with PVT/OpenIPC. In simple terms, it acts as a bridge between a host system and a target platform. It is a very low-cost alternative to most of the other JTAG probes but does have some limited capability.	UTAG - USB JTAG Probe - Debug Tools Support - Intel Enterprise Wiki

26.10.1. Box Stress Tool

BST is an AIO integrated solution used for Voltage measurements, Voltage drive/margining, GPIO's manipulations, I2C master controller and Thermal Diodes measurements capabilities.

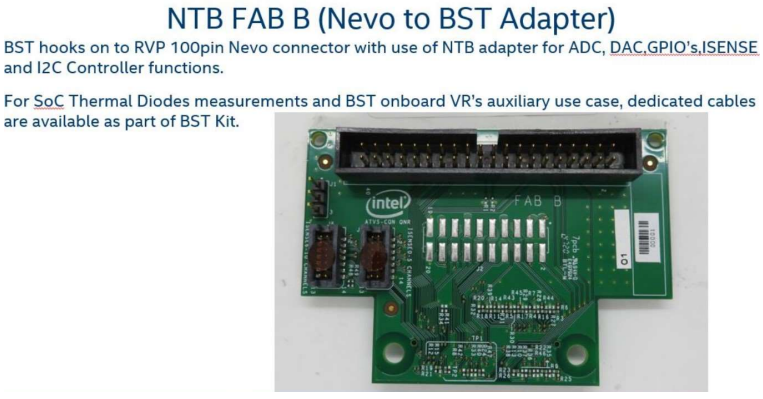


Figure 26-10: Nevo to BST Adapter

Note: Users who want to use Nevo will need an Adapter card and extension cable.

Cable and extension adapter are part of Nevo demand call catalog which open every Quarter, kindly look at info below.

Figure 26-11: Nevo Extension Cable

26.10.1.1. Interface

BST hooks on to RVP 100pin Nevo connector with use of NTB adapter for ADC, DAC, GPIO's and I2C Master functions.

For SoC Thermal Diodes measurements and BST onboard VR's auxiliary use case, dedicated cables will be available as part of BST Kit.

26.10.1.2. Power Supply

For standard operation of ADC, DAC, GPIO's, I2C Master and Thermal diodes measurements the BST is powered from an USB Type-A to uUSB (5V from Host PC to BST).

For BST auxiliary use case a standard ATX with 12V/5V connector is required.

26.10.2. SINAI to CPU sideband optimization

PECI Circuit in RVP has remained legacy and not changed much over many RVP generation.

Refer Existing Implementation.

Current Status:

1. PECI hardware signal is only an internal validation used by thermal teams (INTEC)
2. OOB PECI is not POR and inband **PECI over eSPI** is POR from SOC to EC.
3. EC & SINAI no longer needed PECI dedicated pin connection. InTEC is the only load on the PECI bus.

Proposal (Implementation from PTL onwards):

1. Retain the 3pin 100mil header & remove the PECI MUX circuit completely.
2. Default SoC PECI connection should be pull-down, InTEC users must remove the jumper while validating using InTEC tool.
3. Unstuff the PECI copy/probing circuit as this is not used currently per INTEC users.
4. Retain EC connection to 3 pin header using resistor STUFF option to support any use-case.
5. PECI probing circuit is currently UNSTUFF in PTL and it can be removed from next program onwards, if no use-case is identified from any of the users. (TBD)
6. SINAI connector will have 3V3 level of SoC FORCEPR and THERMTRIP signal.

Teams aligned:

- Kravtsov, Alex1; Ziserson, Alexander (iVE); Littrell, Jeremy D (PPV); Dayan, Rami (QnR)

26.10.2.1. SINAI to CPU sideband implementation

SINAI to CPU sideband implementation in NVL RVP will be as below:

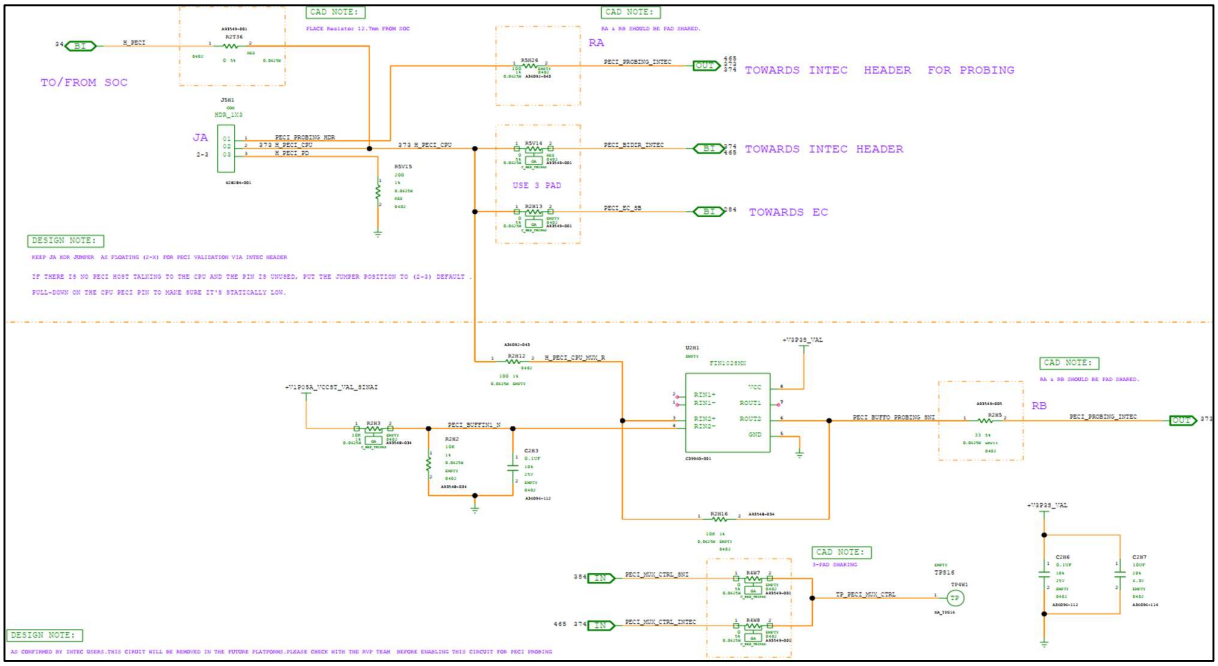


Figure 26-12: SINAI to CPU sideband implementation in NVL (1/2)

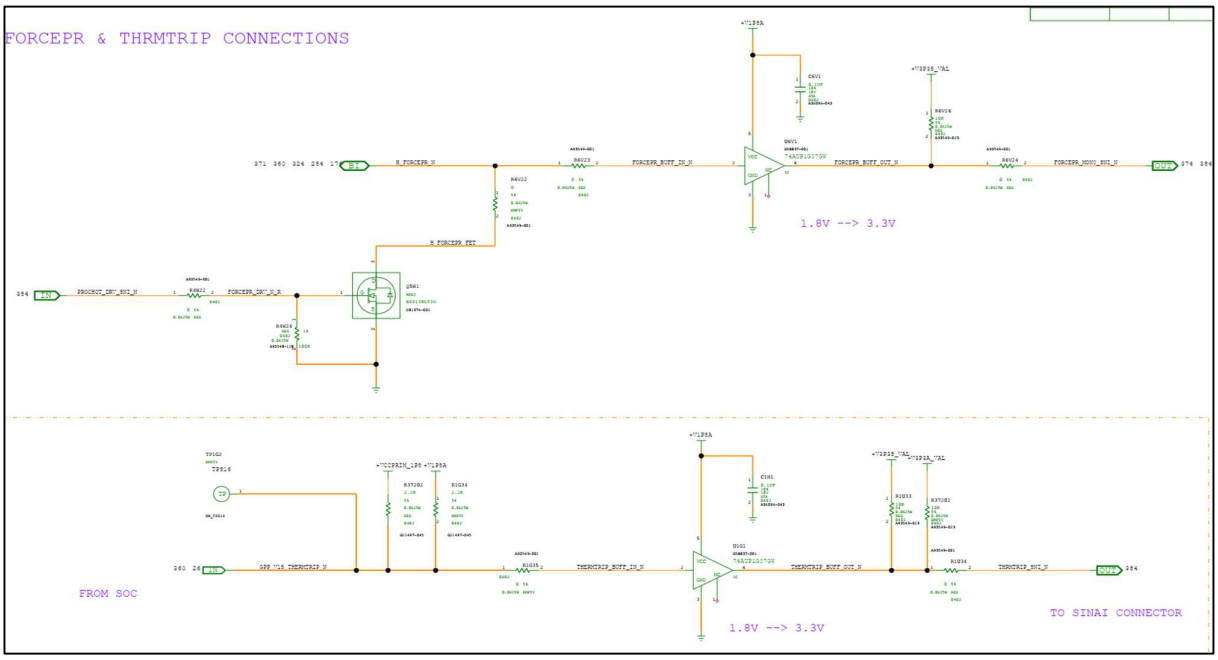


Figure 26-13: SINAI to CPU sideband implementation in NVL (2/2)

26.11. Side Band signals (CPU and EC)

Sideband signals on a platform are used for low-bandwidth, out-of-band communication between different components. They typically handle control messages, status updates, and other auxiliary functions that are not part of the main data path.

Following sideband signals will be supported by NVL RVP.

SOC Side band signals:

FORCEPR_B: The FORCEPR# (Force Power Reduction) signal is an I/O pin related to power and thermal management. It allows external agents to force the processor to enter a low-power state or reduce its power consumption.

VRALERT_B: VRALERT# is a signal used for power and thermal management, particularly related to the voltage regulator (VR). Here is a detailed explanation of VRALERT#

As an Input: VRALERT# is an input pin to the PCH or other system management controllers. It is used by the VR to signal the system that an over-current or thermal event has occurred, requiring immediate action to prevent damage or instability.

Triggering Throttling: When asserted, VRALERT# typically triggers the system to throttle the CPU to the most severe throttling level (Throttle Level 3). This is done to quickly reduce power consumption and mitigate the event that triggered the alert.

EPD_ON*: The EPD_ON (Early Power Down) signal is used in Intel platforms to manage power states and ensure proper coordination between various components during power sequencing.

PECI: The Platform Environment Control Interface (PECI) is a one-wire bus interface that provides a communication channel between Intel processors and chipset components to external monitoring or control devices. PECI allows platform devices to access MSRs and PCI CSRs using the PECI protocol.

CATERR_B: The CATERR# signal is used to indicate catastrophic errors that occur within the system. These errors are severe enough that they require immediate attention and often lead to system reset or shutdown to prevent data corruption or hardware damage.

THERMTRIP_B: The THERMTRIP# (Thermal Trip) signal is a crucial hardware signal used to indicate that the processor or another component has exceeded its maximum safe operating temperature, necessitating an immediate shutdown to prevent damage.

CPU_C10_GATE_B: The CPU_C10_GATE# signal is used to manage power gating for power efficiency during low power states. The CPU_C10_GATE# signal is connected to the Embedded Controller (EC) to perform power management and system coordination. Some of the functions are as follows.

- Coordinated Power Management: Ensures that the EC is aware of the CPU's power state and can manage power rails and VRs accordingly.
- Efficient Power Saving: Optimizes power savings, extending battery life and reducing overall power consumption.
- System Stability and Coordination: Ensures smooth transitions between power states and coordinates wake-up processes.
- Platform Policies and Configuration: Allows customization of power management behavior to meet specific platform needs.
- Integration with Other Signals: Provides a unified power management interface and interacts with other power signals for comprehensive control.

EC Side band signals:

Thermistor input to EC: The Embedded Controller (EC) in a platform typically receives various thermal inputs to manage the system's thermal performance effectively. These thermal inputs help the EC make informed decisions about cooling, power management, and overall system stability. Here are the primary thermal inputs to the EC:

- PCH Temperature Data: Received via eSPI.
- SoC Temperature Data: Includes DTS data sent via IOSF-SB messages.
- VR Temperature Data: Monitored directly or through intermediary components.
- External Sensor Data: Includes discrete sensors communicating over I2C or SMBus.
- Processor Thermal Data: Received via PECI interface and processor signals like PROCHOT# and THERMTRIP#.
- PCIe Device Thermal Data: Monitored from PCIe devices through dedicated channels.
- Battery Temperature Data: Provided by the BMS over SMBus.
- Thermal Trip and Alerts: Include critical thermal signals for immediate action.
- Thermal data for RAM (DRAM/DIMM) through intermediary components.

CPU Fan control signals: The EC uses various signals and mechanisms to regulate fan speeds and ensure adequate cooling based on thermal inputs from various sensors. Here are the key fan control signals and mechanisms used by the EC:

1. PWM Signals: The EC typically uses PWM signals to control the speed of the fans. The duty cycle of the PWM signal determines the fan speed, with a higher duty cycle resulting in higher fan speed.
2. Tachometer (Tach) Feedback Signals: Fans equipped with tachometer outputs provide feedback on their actual speed (RPM). The EC monitors these tach signals to ensure that fans are operating at the desired speeds.
3. Temperature Sensor Inputs:

Thermal Data: The EC receives thermal data from various sensors (e.g., CPU, PCH, VRs, memory, discrete sensors) to determine the cooling needs.

Following diagram captures the Sideband signal implementation on NVL RVP.

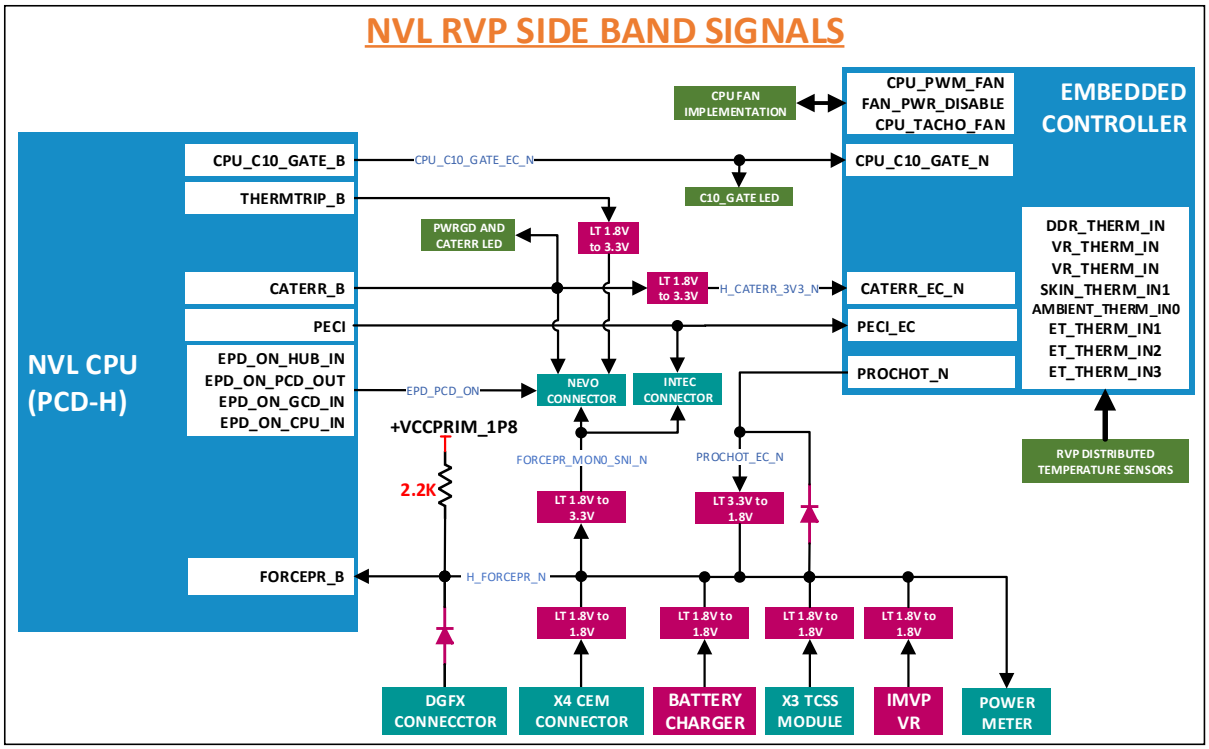


Figure 26-14: NVL RVP Sideband signal implementation.

26.12. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

27. Power and Performance

27.1. Overview

RVP team will follow all the requirements which are mentioned in NVL Power and Performance requirements document (Link). RVP also follows PnP PMR BKM to select the resistors MPNs.

27.2. Voltage margining

For the power and performance validation, margining is supported through Sinai Nevo connector and range of voltages supported are tabulated below. For PCH rails a separate VAL VR (TBD) is provided for margining.

Table 123: Voltage Margining support on NVL RVP (TBD)

NVL Ax SOC Voltage Regulator	VR controller	Nominal Voltage	Voltage range support by VR	Iccmax	Margining Support
+V3P3A	TPS51285A	3.3V	2.97V to 3.63V	TBD	Yes
+V1P8A	RT6220AGQUF	1.8V	0.6V to 5.0V	6A	Yes
+VNNAON	AOZ23567BQI	0.77V	0.6V to 16V	37A	Yes
+VCCIO	TPS51375L	1.25V	0.6V to 5.5V	12A	Yes
+VDD1	TPS51375L	1.8V	0.6V to 5.5V	12A	Yes
+VDD2H	AOZ23567BQI	1.065V (TBD)	0.6V to 16V	37A	Yes
+VDD2L	TPS51375L	0.92V (TBD)	0.6V to 5.5V	12A	Yes
+VDDQ	NB792GD	0.52V/ 0.32V	0.52V/ 0.32V (+/- 10%)	8A	Yes
+VCC1P2_RTC	TPS7A0312DQNR	1.2V	0.8V to 3.3V	1A	Yes
+V0.85A	TPS51219	0.85V	0.5V to 2V	TBD	Yes
+V1.25A	TPS62826DMQR	1.25V	0.6V to 2V	3A	Yes

27.3. Additional Current support

The IMVP VCC_CORE, VCCGT, VCCNPU, VCCSA and VCC_LPECORE VRs support 20% (TBD) more than **PL2** to support stress test.

The teams doing stress tests (that draw higher currents than POR PL2) are expected to have external cooling (maybe an external cooling fan) for VRs. Thermal solution on board does not support cooling requirements during stress tests for higher currents.

IMVP VR's (VCCORE, VCCGT, VCCNPU, VCCSA and VCC_LPECORE) supports POR PL4 current numbers only.

27.4. PnP PMR resistor

2x7 headers are provided on board which brings out voltage and current sense points from the board that can be used for Power and Performance measurement of different power rails for both PCH and CPU and different on-board interfaces. Few of 2x7 connection pairs are left spare, provision to wire for additional measurements on board.

SoC/PCH and CPU current sense lines from Power Measurement Resistor (PMR) are connected to dedicated 2x7 headers. 2x7 HDRs mapping to PMR resistors is available in LINK. CPU and PCH rails assigned/grouped to 2x7 HDRs to optimize the cable connections to NI DAQ.

Special attention from PnP (CPU, SoC/ PCH & ROP PnP) team is required on selection of the PMRs used in NVL Ax RVP. Approach in NVL-Ax RVP is to use the PMRs from the different vendors having same pad dimension, tolerance and temperature coefficient.

List of PMR's supported for NVL Ax SoC, PCH IOE and DRAM are available in LINK.

27.4.1. PnP PMR/Current Sense Resistors Stuffing

As part of cost optimization on NVL RVPs, PMRs/Current Sense Resistors are stuffed and fully supported only on PnP SKUs. In non-PnP SKUs, Current Sense Resistors are partially supported. In non-PnP SKUs, PnP PMRs are provided for those rails which are connected to Power Accumulator Devices only. The rest of sense resistors will be replaced with shorting resistors/copper shunt resistors. The details of each sense resistor which will be converted to the shorting resistor in non-PnP SKUs is captured in excel document available at *LINK*

27.5. Power Accumulator

PAC1954 based power accumulators are provided for measuring power or energy telemetry and PAC1952 based power accumulator for SOC voltage measurement.

Each power accumulator has 4/2 channels (PAC1954 / PAC1952), Per Channel 48-Bit Power Accumulators Capture 17 Minutes of Data at 1024sps. The data can be read through PCD-H I2C bus.

The details of power and energy telemetry mapping of different SKUs are also available at power meter wiki LINK List of rails having the provision for power accumulator will be updated in the HAS1.0 version.

27.6. Test plan link (RVP/ SIV)

Link: will be updated in the HAS1.0 version.

28. RVP Health DAC

28.1. Overview

RVP Health DAC (Debug Acceleration card) is a novel approach that facilitates faster remote debug monitoring & root cause of platform issues. It gives a completely new dimension to diagnostics, remote platform access and validation. It's a pluggable kit solution, which reduces main platform design dependency. The DAC (Debug acceleration card) does not need any special header to connect on RVPs. The overhead is avoided by using existing headers to tap the signals from RVP to provide all the features. This salient unique feature of DAC makes it scalable across all the RVP segments of S, P, M and atom segment N too.

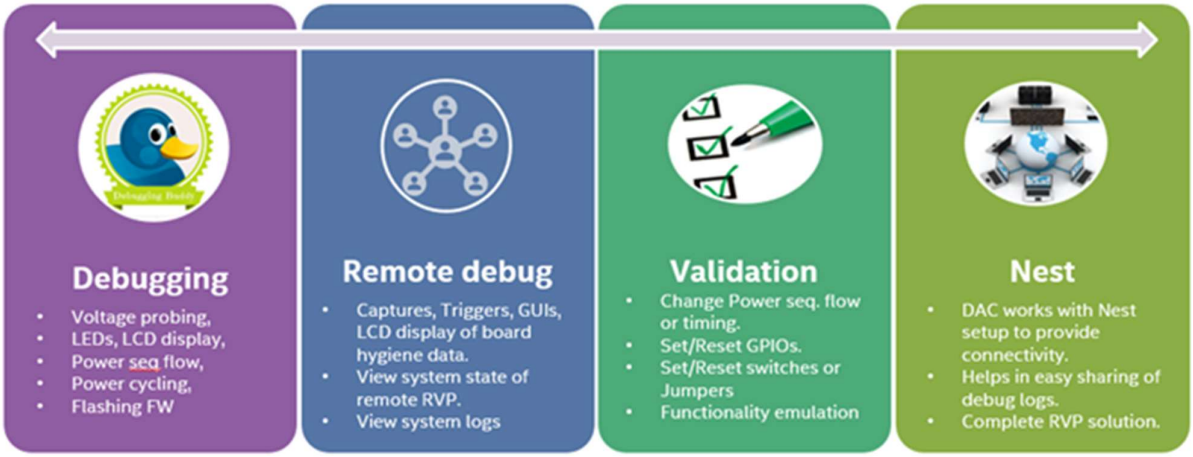


Figure 100: Strategy for debug acceleration card

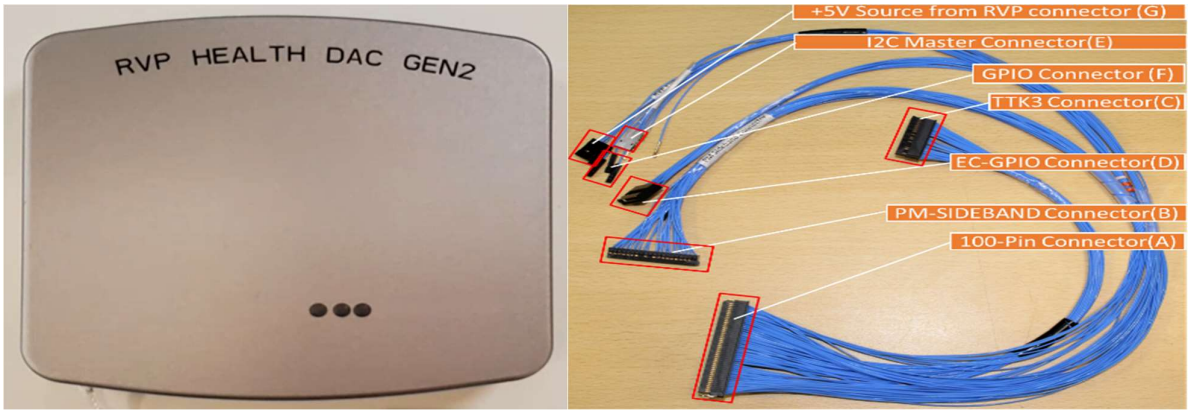


Figure 102: Snapshot of RVP DAC with Cable

For more info on RVP Health DAC, please refer below links:

- RVP DAC goto link: https://goto.intel.com/rvpdac
- RVP DAC Sharepoint: https://intel.sharepoint.com/sites/ccgcpecpsrvpdaconestop
- RVP DAC HAS: RVP Health DAC HAS Template
- Link to Intro video: DAC_Introduction.mp4
- Link to User Guide: RVP_DAC_UG_Gen2_REV1p0.docx

29. UCP-SQUID

29.1. Overview

UCP SQUID is one tool supporting programming over SPI, I2C, SWD and JTAG. It also has GPIOs that connect to Front Panel HDR of RVP and help to get or set the system states. UCP SQUID also has tiny paddle boards and cables designed for needs of Intel RVPs as part of Hardware KIT. The paddle boards host FET devices which enable for systems to boot with UCP SQUID programmer connected to the platform, thus enabling the remote programming hardware tool for Validation teams.

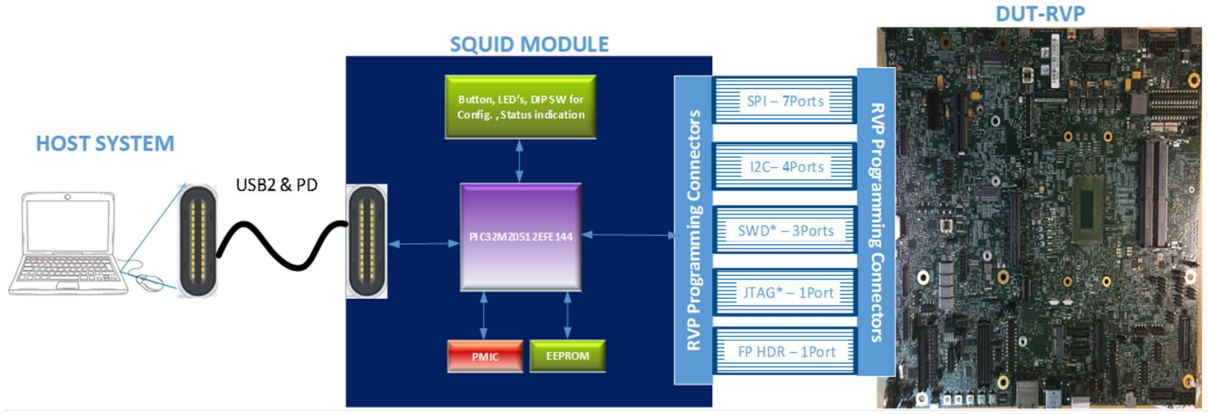


Figure 29-1: UCP-Block diagram

More details about UCP SQUID can be accessed at below link:

- UCP_SQUID_Abstract_Demo.pptx
- CCG-CPE-CPS_UCP-SQUID - Documents - All Documents (sharepoint.com)
- UCP RVP HAS: UCP_SQUID_RVP_HAS

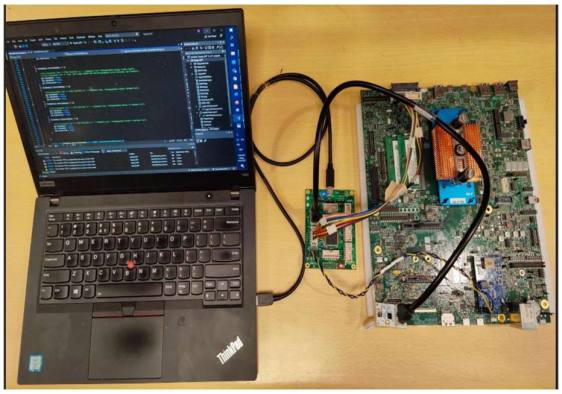
PLATFORM VALIDATION SETUP WITHOUT UCP SQUID	PLATFORM VALIDATION SETUP WITH UCP SQUID
	

Figure 29-2: Snapshot of UPC Squid setup

30. RVP NEST

30.1. Overview

RVP NEST is a remote access farm hosted and maintained by RVP Team. Goal of RVP NEST is to enable early access to platform for the RVP users. RVP NEST gives the in-lab user experience and allows to remotely control the RVP by logging-in through Host PC.

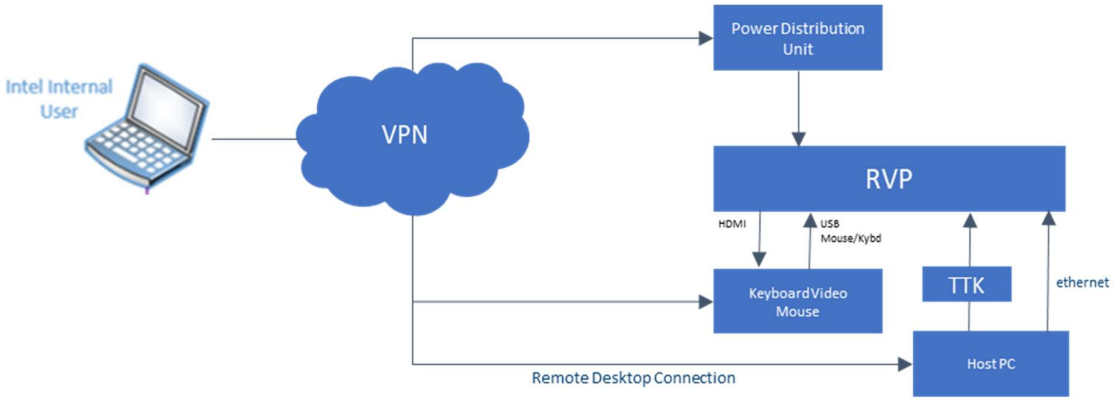


Figure 30-1: RVP NEST Connection diagram

By default, each setup has dedicated host in which KVM, IFWI flashing tool (e.g. TTK3 or DAC or UCP), BIOS serial cable, G3 Cycling support through IP PDU connected to RVP. On need basis, we shall support.

- Setups can be made fully loaded GC or DC configs.
- ITP-XDP debug tools shall be connected.
- Flexible to any OS (Ubuntu/Centos/SVOS) on SUT.
- Peripherals/3PE shall be connected.
- Debug Acceleration Card (DAC) can be connected to platform, UCP, CBS.
- Support post PRQ.
- Optional/Feature Reworks will be supported.

For more details on the RVP Nest User Guide, please visit the below wiki link: https://goto.intel.com/rvpnestwiki

31. Mechanical

31.1. Form Factor

The NVL AX/AM form factor board size: **12”x 10”**, Board Mounting holes will follow ATX requirements (picture below) A, B, C, F, G, H, J, are included by default, availability of R & S Holes are dependent on Layout. If R & S Holes can’t be accommodated, we will provide additional mounting holes wherever necessary based on structural requirement

Each of the holes will follow the standard ATX Mounting Hole spec. (Diameter-156mils) & KoZ.

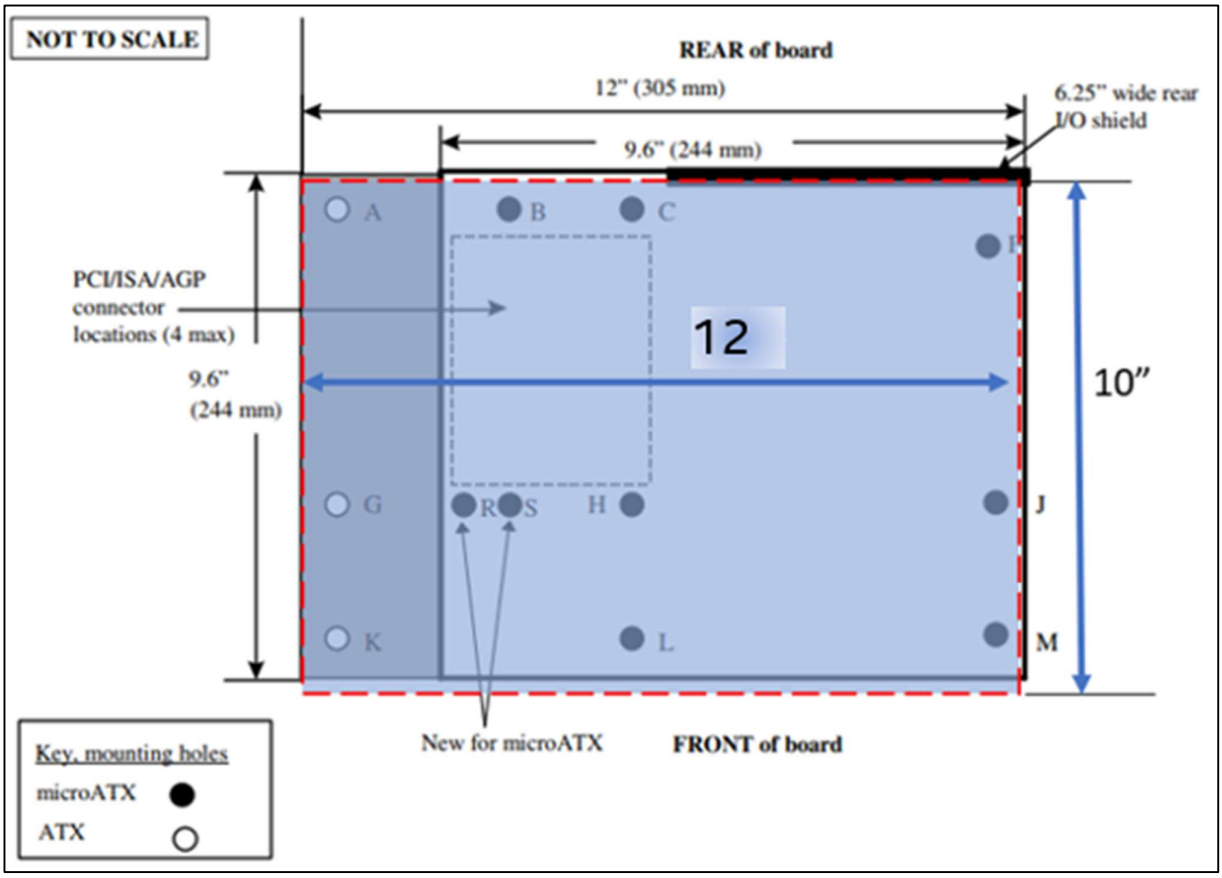


Figure 31-1: AX/AM RVP form factor

Table 124: Form factor dimension

Board name	Form factor dimension
NVL AX/AM RVP	X-Y: 12Inches x 10Inches

32. Chrome Requirement

32.1. Overview

No Chrome Support on NVL AX/AM RVP

33. Regulatory & Product Ecology

The following items must be satisfied to meet regulatory and ecology requirements for the NVL RVP.

- An unauthorized device label needs to be attached/tied to the RVP board at the factory. Intel part number K21553-003 (or later) should be used.
- A safety flyer must be shipped with the RVP board. Intel part number J10643-003 should be used, and the flyer should be included in the packaging box of RVP board.
- Review batteries (including coin cell) being shipped/used with the RVP for proper shipping and safety compliance. The following certificates should be obtained in cooperation with SSC (MSO): UN38.3/MSDS/1.2m drop, CSTCG (Dangerous good), CB (IEC62133), UL1642, REACH SVHC, and EU battery directive. Please refer to DocLocator document "Battery Selection and Approval Procedure" DL-0002566 (legacy SNAP 227-0029), for details.
- Review power supply being shipped/used with the RVP for safety and energy efficiency compliance in the region it is being shipped. For previous RVPs, power supplies with NRTL certification and US Dept. of Energy Level VI efficiency rating have been used. Please refer to DocLocator document "Mains Connected Power Supply Selection and Approval Procedure" DL-0002565 (legacy SNAP 227-0028), for details.
- Intel Pre-lease Loan Agreement (IPLA) "One Pager" must be shipped with the RVP board. It communicates the important legal information about the DV to customer. Intel part number M21973 should be used and included in the packaging box of RVP board.
- When shipping with a battery, there needs to be a battery warning label on the packaging. Li Metal Battery Warning Label (including coin cell if shipped from China): IPN: J72126-004 and/or Li Ion Battery Warning Label: IPN: J72128-004.
- The RVP BOM needs to be reviewed and undergo a risk assessment by a Product Ecology Engineer and given a ship approval. The results will be documented in the product regulatory plan.
- Ecology labeling needs to be attached to the packaging to show compliance to CA perchlorate requirements. Perchlorate label, (sample IPN: D85237-001), needs to be affixed to the packaging of the board containing coin cell battery shipping to CA. Please refer to DocLocator document DL-0002372 "Environmental Product Content Specification for Suppliers & Outsourced Manufacturers" (legacy SNAP 18-1201), 3.5 for details.
- Review components containing laser emitters for eye safety compliance before usage. shall follow distribution requirements outlined in the Laser Regulatory and Product Safety Requirements DL-0002555 (legacy SNAP 227-0009).

- Review radio (Wi-Fi, WiGig, cellular, BT, NFC, etc.) components for regulatory staging and carrier access compliance in the regions it will be used in.
- Complete radiated emissions (EMI) scans to the limits of the regions it will be shipped to ensure no harmful interference (shall be performed with assistance from the PRE). A schematic and layout review for EMC and RF by PRE is recommended.
- Undergo a Safety Review by a qualified Product Regulations Engineer (PRE) or 3rd party certified safety testing organization and found to be "reasonably safe" as defined in the Intel Corporation “Product Regulations Methodology Specification”, DL-0002650 (legacy SNAP 227-GS0021). The criteria used for the safety review are based on the current version of “Information Technology Equipment - Safety”, IEC 62368 or other relevant product specific safety standard.

  DocLocator documents can be found here: https://doclocator.intel.com/