Smarc

User Manual

HALLEY

SMARC® Rel. 2.1.1 compliant module with the Intel® Atom™ x6000E Series and Intel® Pentium® and Celeron® N and J Series processors (formerly Elkhart Lake) for FuSa applications

www.seco.com

REVISION HISTORY

Revision	Date	Note	Rif
1.0	19th April 2021	First official release	AR
1.1	23rd December 2021	Safety Policy included	SO
1.2	26th August 2022	BIOS documentation	SO
1.3	13th April 2023	Included engineering samples policy Included decoupling circuit for HDMI 1.4	SO

Every effort has been made to ensure the accuracy of this manual. However, SECO S.p.A. accepts no responsibility for any inaccuracies, errors or omissions herein. SECO S.p.A. reserves the right to change precise specifications without prior notice to supply the best product possible.

For further information on this module or other SECO products, but also to get the required assistance for any and possible issues, please contact us using the dedicated web form available at http://www.seco.com (registration required).

Our team is ready to assist.

INDEX

Chapter 1.
INTRODUCTION

- Warranty
- Information and assistance
- RMA number request
- Safety
- Electrostatic Discharges
- RoHS compliance
- Terminology and definitions
- Reference specifications

1.1 Warranty

This product is subject to the Italian Law Decree 24/2002, acting European Directive 1999/44/CE on matters of sale and warranties to consumers.

The warranty on this product lasts for 1 year.

Under the warranty period, the Supplier guarantees the buyer assistance and service for repairing, replacing or credit of the item, at the Supplier’s own discretion.

Shipping costs that apply to non-conforming items or items that need replacement are to be paid by the customer.

Items cannot be returned unless previously authorised by the supplier.

The authorisation is released after completing the specific ticketing procedure https://support.seco.com/ (web RMA). The RMA authorisation number must be put both on the packaging and on the documents shipped with the items, which must include all the accessories in their original packaging, with no signs of damage to, or tampering with, any returned item.

The error analysis form identifying the fault type must be completed by the customer and has must accompany the returned item.

If any of the above-mentioned requirements for RMA is not satisfied, the item will be shipped back and the customer will have to pay any and all shipping costs.

Following a technical analysis, the supplier will verify if all the requirements, for which a warranty service applies, are met. If the warranty cannot be applied, the Supplier will calculate the minimum cost of this initial analysis on the item and the repair costs. Costs for replaced components will be calculated separately.

SECO offers Engineering Samples for early evaluation and development. Engineering Samples are sold “as-is” with no warranty of any kind, neither explicit nor implied.

Here https://www.seco.com/it/EngineeringSamplesPolicy is defined the framework of SECO and customer responsibilities regarding Engineering Samples.

⚠ Warning!
All changes or modifications to the equipment not explicitly approved by SECO S.p.A. could impair the equipment’s functionality and could void the warranty

1.2 Information and assistance

What do I have to do if the product is faulty?

SECO S.p.A. offers the following services:

- SECO website: visit http://www.seco.com to receive the latest information on the product. In most of the cases it is possible to find useful information to solve the problem.
- SECO Sales Representative: the Sales Rep can help to determine the exact cause of the problem and search for the best solution.
- SECO Help-Desk: contact SECO Technical Assistance. A technician is at disposal to understand the exact origin of the problem and suggest the correct solution.

  E-mail: technical.service@seco.com

  Fax (+39) 0575 350210

- Repair center: it is possible to send the faulty product to the SECO Repair Centre. In this case, follow this procedure:
  - Returned items must be accompanied by a RMA Number. Items sent without the RMA number will be not accepted.
  - Returned items must be shipped in an appropriate package. SECO is not responsible for damages caused by accidental drop, improper usage, or customer neglect.

Note: Please have the following information before asking for technical assistance:

- Name and serial number of the product;
- Description of Customer's peripheral connections;
- Description of Customer's software (operating system, version, application software, etc.);
- A complete description of the problem;
- The exact words of every kind of error message encountered.

1.3 RMA number request

To request an RMA number, please visit SECO's web-site. On the home page, please select "RMA Online" and follow the procedure described.

An RMA Number will be sent within 1 working day (only for on-line RMA requests).

1.4 Safety

This board uses only extremely low voltages.

While handling the board, please use extreme caution to avoid any kind of risk or damages to electronic components.

!

Always switch the power off, and unplug the power supply unit, before handling the board and/or connecting cables or other boards.

Avoid using metallic components - like paper clips, screws and similar - near the board when connected to a power supply, to avoid short circuits due to unwanted contacts with other board components.

If the board has become wet, never connect it to any external power supply unit or battery.

Check carefully that all cables are correctly connected and that they are not damaged.

1.5 Electrostatic Discharges

This board, like any other electronic product, is an electrostatic sensitive device: high voltages caused by static electricity could damage some or all the devices and/or components on-board.

!

Whenever handling this product, ground yourself through an anti-static wrist strap. Placement of the board on an anti-static surface is also highly recommended.

1.6 RoHS compliance

This board is designed using RoHS compliant components and is manufactured on a lead-free production line. It is therefore fully RoHS compliant.

1.7 Safety Policy

In order to meet the safety requirements of EN62368-1:2014 standard for Audio/Video, information and communication technology equipment, the HALLEY module shall be:

- used inside a fire enclosure made of non-combustible material or V-1 material (the fire enclosure is not necessary if the maximum power supplied to the module never exceeds 100 W, even in worst-case fault);
- used inside an enclosure; the enclosure is not necessary if the temperature of the parts likely to be touched never exceeds 70 °C;
- installed inside an enclosure compliant with all applicable IEC 62368-1 requirements;

The manufacturer which includes a HALLEY module in his end-user product shall:

- verify the compliance with B.2 and B.3 clauses of the EN62368-1 standard when the module works in its own final operating condition
- Prescribe temperature and humidity range for operating, transport and storage conditions;
- Prescribe to perform maintenance on the module only when it is off and has already cooled down;
- Prescribe that the connections from or to the Module have to be compliant to ES1 requirements;
- The module in its enclosure must be evaluated for temperature and airflow considerations.

1.8 Terminology and definitions

ACPI	Advanced Configuration and Power Interface, an open industrial standard for the board’s devices configuration and power management
AHCI	Advanced Host Controller Interface, a standard which defines the operation modes of SATA interface
API	Application Program Interface, a set of commands and functions that can be used by programmers for writing software for specific Operating Systems
AVC	Advanced Video Coding, a video compression standard, also known as H.264
BIOS	Basic Input / Output System, the Firmware Interface that initializes the board before the OS starts loading
CAN Bus	Controller Area network, a protocol designed for in-vehicle communication
DDC	Display Data Channel, a kind of I2C interface for digital communication between displays and graphics processing units (GPU)
DDR	Double Data Rate, a typology of memory devices which transfer data both on the rising and on the falling edge of the clock.
DP	Display Port, a type of digital video display interface
eDP	embedded Display Port, a type of digital video display interface developed especially for internal connections between boards and digital displays
GBE	Gigabit Ethernet
Gbps	Gigabits per second
GND	Ground
GPI/O	General purpose Input/Output
HEVC	High Efficiency Video Coding, a video compression standard, also known as H.265
HD Audio	High Definition Audio, most recent standard for hardware codecs developed by Intel® in 2004 for higher audio quality
HDMI	High Definition Multimedia Interface, a digital audio and video interface
I2C Bus	Inter-Integrated Circuit Bus, a simple serial bus consisting only of data and clock line, with multi-master capability
I2S	Inter-Integrated Circuit Sound, an audio serial bus protocol interface developed by Philips (now NXP) in 1986
JPEG/MJPEG	Joint Photographic Experts Group, standard method for lossy compression of digital images. Motion JPEG is a video compression format
LAN	Local Area Network
LPDDR4	Low-Power Double Data Rate Synchronous Dynamic Random Access Memory, 4th generation
LVDS	Low Voltage Differential Signalling, a standard for transferring data at very high speed using inexpensive twisted pair copper cables, usually used for video applications
Mbps	Megabits per second
MIPI	Mobile Industry Processor Interface alliance
MMC/eMMC	MultiMedia Card / embedded MMC, a type of memory card, having the same interface as the SD card. The eMMC is the embedded version of

	the MMC. They are devices that incorporate the flash memories on a single BGA chip.
MPEG2	Standard for the generic coding of moving pictures and associated audio information
MVC	Multiview Video Coding, a stereoscopic video coding standard for video compression
N.A.	Not Applicable
N.C.	Not Connected
OpenCL	Open Computing Language, specifies programming languages for programming different devices and API
OpenGL	Open Graphics Library, an Open Source API dedicated to 2D and 3D graphics
OpenVG	Open Vector Graphics, an Open Source API dedicated to hardware accelerated 2D vector graphics
OS	Operating System
PCI-e	Peripheral Component Interface Express
PHY	Abbreviation of Physical, it is the device implementing the Physical Layer of ISO/OSI-7 model for communication systems
PWM	Pulse Width Modulation
PWR	Power
RGMII (PHY)	Reduced Gigabit Media Independent Interface, a standard interface between the Ethernet Media Access Control (MAC) and the Physical Layer
SATA	Serial Advance Technology Attachment, a differential full duplex serial interface for Hard Disks
SD	Secure Digital, a memory card type
SDIO	Secure Digital Input/Output, an evolution of the SD standard that allows the use of the same SD interface to drive different Input/Output devices, like cameras, GPS, Tuners and so on.
SGET	Standardization Group for Embedded Technologies
SMARC	Smart Mobility Architecture, a computer Module standard maintained by the SGET
SM Bus	System Management Bus, a subset of the I2C bus dedicated to communication with devices for system management, like a smart battery and other power supply-related devices.
SOC	System-on-a-chip
SPI	Serial Peripheral Interface, a 4-Wire synchronous full-duplex serial interface which is composed of a master and one or more slaves, individually enabled through a Chip Select line.
TBM	To be measured
TMDS	Transition-Minimized Differential Signalling, a method for transmitting high speed serial data, normally used on DVI and HDMI interfaces
UART	Universal Asynchronous Receiver-Transmitter, is an asynchronous serial interface where data format and transmission speed are configurable
UEFI	Unified Extensible Firmware Interface, a specification defining the interface between the OS and the board's firmware. It is meant to replace the original BIOS interface

USB	Universal Serial Bus
VP8	Open video compression format, a traditional block-based transform coding format
VP9	Successor to VP8, customized for video greater than 1080p
WMV9	Series 9 of Windows Media Video, a video compression format inlcuding native support for interlaced video, non-square pixels, and frame interpolation

1.9 Reference specifications

Here below it is a list of applicable industry specifications and reference documents.

Reference	Link
ACPI	https://uefi.org/specifications
AHCI	http://www.intel.com/content/www/us/en/io/serial-ata/ahci.html
CAN Bus	http://www.bosch-semiconductors.de/en/ubk_semiconductors/safe/ip_modules/can_literature/can_literature.html
DDC	http://www.vesa.org
DP, eDP	http://www.vesa.org
FastEthernet	http://standards.ieee.org/about/get/802/802.3.html
Gigabit Ethernet	https://standards.ieee.org/standard/802_3-2018.html
HD Audio	http://www.intel.com/content/dam/www/public/us/en/documents/product-specifications/high-definition-audio-specification.pdf
HDMI	http://www.hdmi.org/index.aspx
I2C	http://www.nxp.com/documents/other/UM10204_v5.pdf
I2S	https://www.sparkfun.com/datasheets/BreakoutBoards/I2SBUS.pdf
Intel® Atom™ Elkhart Lake family	https://ark.intel.com/content/www/us/en/ark/products/codename/80644/Elkhart-lake.html#@Embedded
LVDS	http://www.ti.com/ww/en/analog/interface/lvds.shtml and http://www.ti.com/lit/ml/snla187/snla187.pdf
MIPI	http://www.mipi.org
MMC/eMMC	http://www.jedec.org/committees/jc-649
OpenGL	http://www.opengl.org
OpenVG	http://www.khronos.org/openvg
PCI Express	http://www.pcisig.com/specifications/pciexpress
SATA	https://www.sata-io.org
SMARC Design Guide 2.0	https://sget.org/wp-content/uploads/2018/09/SMARC_DG_V2.pdf
SMARC Hardware Specification 2.1.1	https://sget.org/wp-content/uploads/2020/05/SMARC_V211.pdf
SD Card Association	https://www.sdcard.org/home

SDIO	https://www.sdcard.org/developers/overview/sdio
SM Bus	http://www.smbus.org/specs
TMDS	http://www.siliconimage.com/technologies/tmds
UEFI	http://www.uefi.org
USB 2.0 and USB OTG	http://www.usb.org/developers/docs/usb_20_070113.zip
USB 3.0	https://usb.org.10-1-108-210.causewaynow.com/sites/default/files/usb_32_20191024.zip

Chapter 2.
OVERVIEW

- Introduction
- Technical Specifications
- Electrical Specifications
- Mechanical Specifications
- Supported Operating Systems
- Block Diagram

2.1 Introduction

HALLEY is a SMARC Rel. 2.1.1 compliant module based on the Intel® Atom® x6000E Series and Intel® Pentium® and Celeron® N and J Series processors (formerly Elkhart Lake) for FuSa applications, a series of Dual / Quad SOCs with 64-bit instruction set.

These new family of processors offers different use conditions, such as PC Client, Embedded and Industrial targets and is optimized for usage in vertical applications for IOT including Industrial, Office Automation, Retail, Gaming, Healthcare, Transportation.

New features introduced by Elkhart Lake are, but not limited to the following: Time Sensitive Network (TSN) and Time Coordinate Computing (TCC) for real-time and responsive applications, Scalability and consolidation of temporally deterministic workloads, In band and OOB remote manageability (reboot/power-on/power-off), Platform Trust Technology (PTT), Dynamic Application Loader (DAL) and Secure Guard Extension (SGX), Intel Programmable Service Engine, Intel UHD Graphics, media, and display supporting, Fully Integrated Voltage Regulator (FIVR). Last but not least, this is the first Intel product designed with functional safety capabilities, made available by Intel® Safety Island (SI), a functional safety IP integrated into the Elkhart Lake Platform Control Hub (PCH), intended to raise the safety level of the platform with a single source for managing the safety faults of the SOC.

These SOCs embed all the features usually obtained by combination of CPU + platform Controller hubs, all in one single IC, which allows, therefore, the system minimisation and performance optimisation, which is essential for boards with sizes so reduced as for SMARC (“Smart Mobility ARChitecture”) form factor, offering the computing abilities of a standard board, with the possibilities of combining with a ready-to-use carrier board like the SECO CSM-B79 or customised carrier board.

The Embedded Memory Controller allows the integration of up to 16GB of LPDDR4 Memory directly soldered onboard with In-Band Error Correction Code supported (Safety related feature) and speed up to 4267MT/s on single rank and 3733MT/s on dual rank.

All SOCs embed an Intel® Gen11 UHD Graphics controller with up to 32 Execution Units, which offer high graphical performances, with support for Microsoft® DirectX12.1, OpenGL 4.5, OpenCL™ 1.2, OpenGL ES 3.1, Vulkan 1.1 and HW acceleration for video encoding and decoding of HEVC (H.265), H.264, VP8, VP9, JPEG/MJPEG. It is also possible the HW video decoding only of MPEG2, VC-1.

This embedded GPU is able to drive three independent displays, by using the interfaces available on SMARC connector: one DP++ 1.4, one HMDI 1.4 or DP++ 1.4 and one eDP 1.3 or Dual Channel 18/24bit LVDS (factory alternatives).

Mass Storage capabilities of the board include one external S-ATA Gen3 channel, a standard 4-bit SD interface and one optional eMMC 5.1 Drive soldered on board (Safety related), with up to 128GB capabilities.

Other than the interfaces already discussed previously, on SMARC connector there are the signals necessary for the implementation of 2x GbE, up to 6 ports in USB2.0 only and up to 2 Super Speed (SS) ports (i.e. USB 3.1 Gen2 compliant), 4 x PCI-Express Gen3 lanes, HD and I²S Audio interfaces, CAN, I²C, SPI and SM buses, up to 14 GPIOs, HS-UART and UART interfaces.

Interfacing to the board comes through a single card edge connector, whose pinout is defined by SMARC specifications Rel.2.1.1. For external interfacing to standard devices, a carrier board with a 230-pin MXM connector is needed. This board will implement all the routing of the interface signals to external standard connectors, as well as integration of other peripherals/devices not already included in HALLEY CPU module.

Please refer to following chapter for a complete list of all peripherals integrated and characteristics.

2.2 Technical Specifications

Processors

Intel® Atom™ x6000E CPUs certified for FuSa, compliant to IEC 61508 and ISO 13849 requirements for Functional Safety and Safety Integrity Levels:

- Atom™ x6427FE Quad Core @1.9GHz (no Turbo) 12W TDP w/ IBECC, IHS and TCC, FuSa Certified - Ind. Temp. Range
- Atom™ x6200FE Dual Core @1.0GHz (no Turbo) 4.5W TDP no Graphics w/ IBECC, IHS and TCC, FuSa Certified- Ind. Temp. Range

Other Intel Atom™ x6000E, Pentium® and Celeron® N and J Series CPUs:

- Celeron® J6413 Quad Core @ 1.8GHz (3.0GHZ Turbo) 10W TDP - Comm. Temp. Range
- Celeron® N6211 Dual Core @1.2GHz (3.0GHZ Turbo) 6.5W TDP - Comm. Temp. Range
- Pentium® J6426 Quad Core @2.0GHz (3.0GHZ Turbo) 10W TDP - Comm. Temp. Range
- Pentium® N6415 Quad Core @1.2GHz (3.0GHZ Turbo) 6.5W TDP - Comm. Temp. Range
- Atom™ x6211E Dual Core @1.3GHz (3.0GHZ Turbo) 6W TDP w/ IBECC and IHS - Ind. Temp. Range
- Atom™ x6413E Quad Core @1.5GHz (3.0GHZ Turbo) 9W TDP w/ IBECC and IHS - Ind. Temp. Range
- Atom™ x6425E Quad Core @2.0GHz (3.0GHZ Turbo) 12W TDP w/ IBECC and IHS - Ind. Temp. Range
- Atom™ x6212RE Dual Core @1.2GHz (no Turbo) 6W TDP w/ IBECC, IHS and TCC - Ind. Temp. Range
- Atom™ x6414RE Quad Core @1.5GHz (no Turbo) 9W TDP w/ IBECC, IHS and TCC - Ind. Temp. Range
- Atom™ x6425RE Quad Core @1.9GHz (no Turbo) 12W TDP w/ IBECC, IHS and TCC - Ind. Temp. Range

(*) IHS: Integrated Heatspreader; TCC: Time Coordinated Computing

Memory

32-bit LPDDR4x Soldered Down Memory
Up to 16GB Quad Channel with In-Band Error Correction Code (IBECC, Safety Related feature) supported
4GB Dual Channel, 8GB or 16GB Quad Channel
Speed:4267MT/s single rank (1GB/2GB/4GB/8GB), 3733MT/s dual rank (16GB)

Graphics

Up to 3 independent displays
Integrated Gen11 UHD Graphics controller with up to 32 EU
4K HW decoding and encoding of HEVC (H.265), H.264, VP8/ VP9, WMV9/VC1 (decoding only)
DirectX 12.1, OpenGL ES 3.1, OpenGL 4.5, OpenCL™ 1.2, Vulkan 1.0

Video Interfaces

eDP 1.3 or Dual Channel 18/24bit LVDS interface (factory options)
2 x DP++ 1.4 or 1x DP++ 1.4 and 1x HDMI 1.4 interfaces

Video Resolution

Up to 4096 x 2160 @60Hz

Mass Storage

1 x external S-ATA Gen3 Channel
SDIO interface
Optional eMMC 5.1 drive soldered on-board (Safety Related)

PCI Express

Up to 4 x PCI-e Gen3 Lanes

Networking

2x Gigabit Ethernet PHY with precision clock synchronization and synchronous Ethernet clock output for IEEE 1588 (Safety Related – Black channel).
Optional SERDES (SGMII) Interface for additional third Gigabit Ethernet (factory option, alternative to fourth PCI-e lane)

USB

6 x USB 2.0 Host Ports
2 x USB 3.1 Gen2 Ports

Audio

HD Audio interface

Serial ports

2 x HS-UARTs (Safety Related)
2 x UARTs

CAN Bus

2 x CAN interfaces

Other Interfaces

Up to 14x GPIOs
SM Bus
Power Management Signals
I2C Bus
1x SPI interface for boot
1x General Purpose SPI or eSPI (Factory Alternatives)

Functional Safety Features

FuSa Interface signals for IEC 61508 and ISO 13849

Power supply voltage: +5V$_{DC}$ and +3.3V_RTC

Operating System

Microsoft® Windows 10 Enterprise (64 bit)
Linux Yocto 64-bit

Operating temperature:

Commercial version 0°C ÷ +60°C **.
Industrial version -40°C ÷ +85°C **.

Dimensions: 50 x82 mm (1.97” x 3.23”)

! *** Measured at any point of SECO standard heatspreader for this product, during any and all times (including start-up). Actual temperature will widely depend on application, enclosure and/or environment. Upon customer to consider application-specific cooling solutions for the final system to keep the heatspreader temperature in the range indicated.*
Please also check paragraph 5.1

2.3 Electrical Specifications

According to SMARC specifications, the HALLEY module needs to be supplied only with an external $+5V_{DC}$ power supply.

For Real Time Clock working and CMOS memory data retention, it is also needed a backup battery voltage. All these voltages are supplied directly through card edge fingers (see connector's pinout). All remaining voltages needed for board's working are generated internally from $+5V_{DC}$ power rail.

2.3.1 Power Consumption

HALLEY module, like all SMARC modules, needs a carrier board for its normal working. All connections with the external world come through this carrier board, which provide also the required voltage to the board, deriving it from its power supply source. Anyway, it has been possible to measure power consumption directly on VDD_IN power rail ($5V_{DC}$) that supplies the board. Power consumption must be intended as average value (30 seconds acquisition).

Status	Configuration															
	Intel Atom™ x6425E 16GB LPDDR4 128GB eMMC 4 x PCI-e LVDS and 2x DP++ TPM 2.0 Comm Temp Range				Intel Pentium® J6425 8GB LPDDR4 128GB eMMC 4 x PCI-e LVDS and 2x DP++ TPM 2.0 Comm Temp Range				Intel Atom™ x6425RE 16GB LPDDR4 128GB eMMC 4 x PCI-e eDP and 2x DP++ TPM 2.0 Ind Temp Range				Intel Atom™ x6427FE 8GB LPDDR4 64GB eMMC 4 x PCI-e LVDS and 2x DP++ TPM 2.0 FuSa Ind Temp Range			
	Avg Value		Peak Value		Avg Value		Peak Value		Avg Value		Peak Value		Avg Value		Peak Value	
Idle – (Win10) – power saving configuration	3.5W	0.7A	6.22W	1.24A	2.46W	0.49A	6.79W	1.35A	6W	1.2A	6.3W	1.26A	6.97W	1.39A	9.71W	1.94A
OS Boot – (Win10)	5.68W	1.13A	12.63W	2.52A	6.28W	1.25A	9.41W	1.88A	7.85W	1.57A	13.6W	2.72A	6.83W	1.36A	12.61W	2.52A
Video reproduction @1080p	4.34W	0.54A	9.96W	2A	4.27W	0.85A	11W	2.2A	6.53W	1.31A	9.12W	1.82A	7.38W	1.47A	9.49W	1.9A
Video reproduction 4K	6.71W	1.34A	10.64W	2.12A	6W	1.2A	11.83W	2.36A	7.76W	1.55A	10.47W	2.09A	7.76W	1.55A	10.47A	2.09A
Intel PTU (package power limit and TURBO Enabled)	16.12W	3.22A	19.96W	3.98A	11.22W	2.24A	16.29W	3.25A	13.68W	2.73A	14.52W	2.9A	13.39W	2.68A	14.03W	2.8A
Intel PTU (without power limits and TURBO Enabled)	22.91W	4.58A	24.2W	4.83A	17.36W	3.47A	18.92W	3.98A	14.46W	2.89A	15.74W	3.15A	14.39W	2.87A	15.6W	3.12A

Independently by the SOC mounted onboard, the following power consumptions are common to all boards:

Battery Backup power consumption:	3.11μA
Soft-Off State power consumption:	174mA
Suspend State power consumption:	176mA

2.3.2 Power Rails meanings

In all the tables contained in this manual, Power rails are named with the following meaning:

VDD_IN: Module power input voltage. +5V voltage directly coming from the card edge connector, internally named as 5V_DSW.

VDD_RTC: Low current RTC circuit backup power. 3V coin cell voltage coming from the edge card for supplying the RTC clock on the Elkhart Lake SOCs.

+3.3V_DSW: +3.3 Deep Sleep Well, derived internally from 5V_DSW

+3.3V_RUN: +3.3 Switched voltage, derived internally from +3.3V_DSW

+3.3V_ALW: +3.3 Always-on voltage, derived internally from +3.3V_DSW

+1.8V_ALW: +1.8 Always-on voltage, derived internally from 5V_DSW

+1.8V_RUN: +1.8 Switched voltage, derived internally from +1.8V_ALW

+1.8V_DSW: +1.8 Deep sleep well, derived internally from +3.3V_DSW

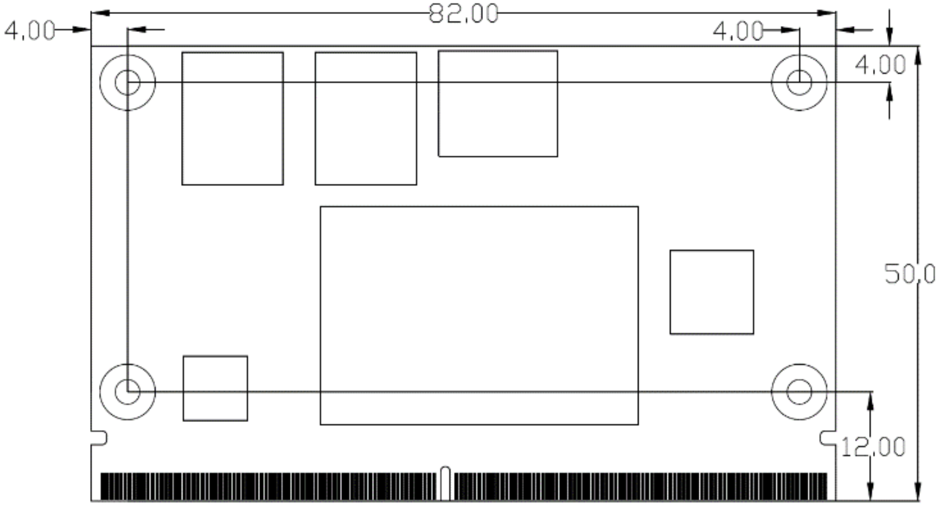
2.4 Mechanical Specifications

According to SMARC® specifications, the board dimensions are: 50 x 82 mm (1.97” x 3.23”) including the pin numbering and edge finger pattern.

Printed circuit of the board is made of twelve layers, some of them are ground planes, for disturbance rejection.

The MXM connector accommodates various connector heights for different carrier board applications needs.

When using different connector heights, please consider that, according to SMARC specifications, components placed on bottom side of the module will have a maximum height of 1.3mm. Keep this value in mind when choosing the MXM connector’s height, if there is the need to place components on the carrier board in the area below the SMARC module.



2.5 Supported Operating Systems

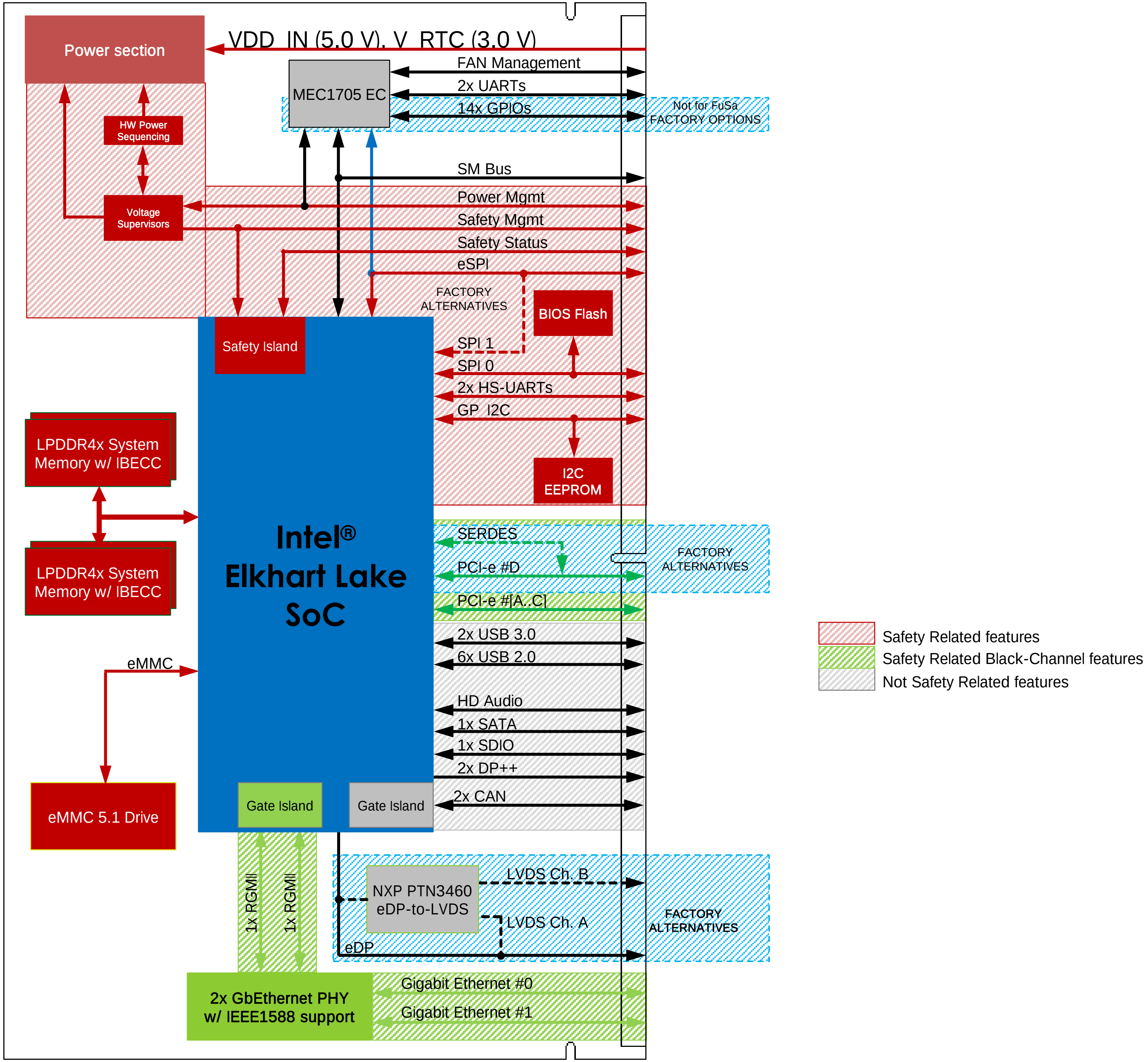
HALLEY module supports the following operating systems:

- Microsoft® Windows 10 Enterprise (64 bit)
- Linux Yocto 64-bit

SECO will offer the BSP (Board Support Package) for these O.Ss, to reduce at minimum SW development of the board, supplying all the drivers and libraries needed for use both with the SMARC board and the Carrier Board, assuming that the Carrier Board is designed following SECO SMARC Design Guide, with the same IC’s.

For further details, please visit https://www.seco.com.

2.6 Block Diagram

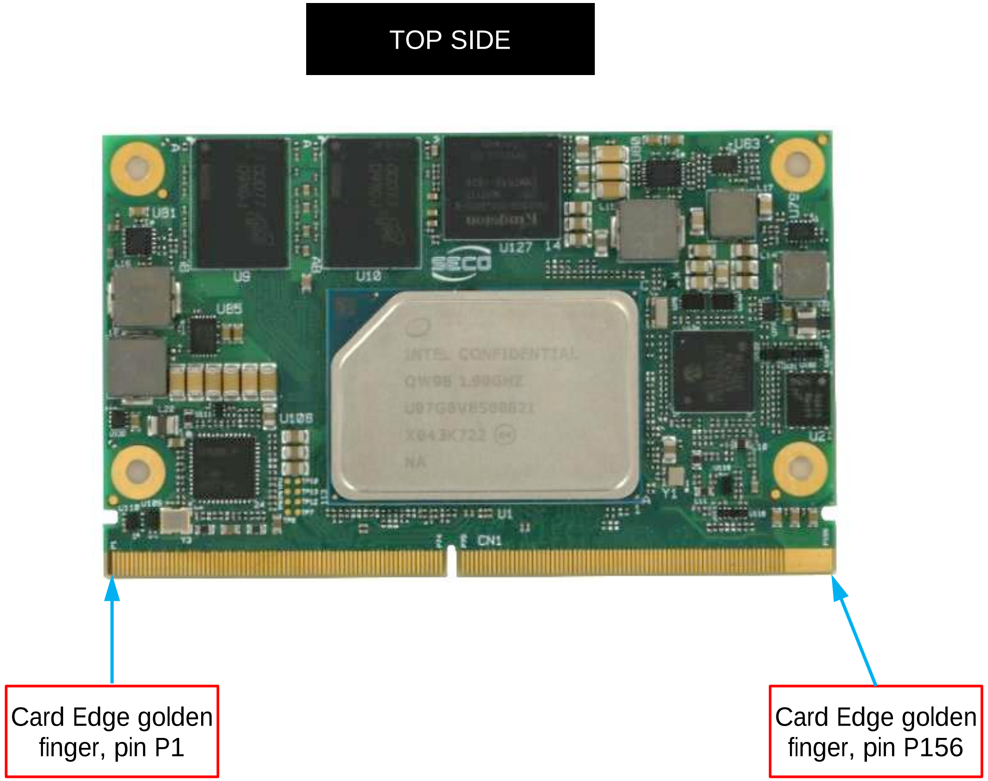


Chapter 3.
CONNECTORS

- Introduction
- Connectors description

3.1 Introduction

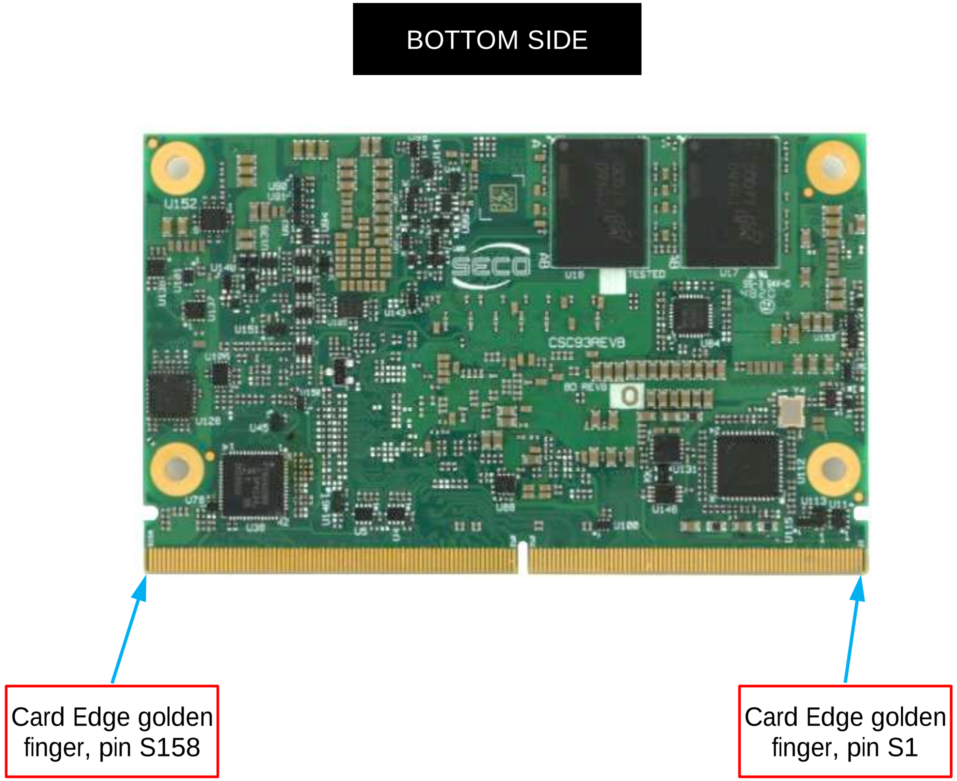
According to SMARC specifications, all interfaces to the board are available through a single card edge connector.



TOP SIDE

Card Edge golden finger, pin P1

Card Edge golden finger, pin P156



BOTTOM SIDE

Card Edge golden finger, pin S158

Card Edge golden finger, pin S1

3.2 Connectors description

3.2.1 SMARC Connector

According to SMARC Rel 2.1 specification, all interface signals are reported on the card edge connector, which is a 314-pin Card Edge that can be inserted into standard low profile 314 pin 0.5mm right pitch angle connector that was originally defined for use with MXM3 graphics cards.

Not all signals contemplated in the SMARC Rel 2.1 are implemented on card edge connector, therefore, please refer to the following table for a list of effective signals reported on the card edge connector.

For accurate signals description, please consult the following paragraphs.

SMARC Golden Finger Connector – CN1							
TOP SIDE				BOTTOM SIDE			
SIGNAL GROUP	Type	Pin name	Pin nr.	Pin nr.	Pin name	Type	SIGNAL GROUP
				S1	PROCHOT	I/O	FUSA
MANAGEMENT	I	SMB_ALERT#	P1	S2	FUSA_PWRFAIL#	I/O	FUSA
		GND	P2	S3	GND		
		N.C.	P3	S4	CHXPMICEN	I	FUSA
		N.C	P4	S5	N.C.		
GBE	I/O	GBE1_SDP	P5	S6	N.C.		
GBE	I/O	GBE0_SDP	P6	S7	N.C.		
		N.C.	P7	S8	N.C.		
		N.C	P8	S9	N.C.		
		GND	P9	S10	GND		
		N.C.	P10	S11	N.C.		
		N.C	P11	S12	N.C.		
		GND	P12	S13	GND		
		N.C.	P13	S14	N.C.		
		N.C	P14	S15	N.C.		
		GND	P15	S16	GND		
		N.C.	P16	S17	GBE1_MDI0+	I/O	GBE

		N.C	P17	S18	GBE1_MDI0-	I/O	GBE
		GND	P18	S19	GBE1_LINK100#	O	
GBE	I/O	GBE0_MDI3-	P19	S20	GBE1_MDI1+	I/O	GBE
GBE	I/O	GBE0_MDI3+	P20	S21	GBE1_MDI1-	I/O	GBE
GBE	O	GBE0_LINK100#	P21	S22	GBE1_LINK1000#	O	
GBE	O	GBE0_LINK1000#	P22	S23	GBE1_MDI2+	I/O	GBE
GBE	I/O	GBE0_MDI2-	P23	S24	GBE1_MDI2-	I/O	GBE
GBE	I/O	GBE0_MDI2+	P24	S25	GND		
GBE	O	GBE0_LINK_ACT#	P25	S26	GBE1_MDI3-	I/O	GBE
GBE	I/O	GBE0_MDI1-	P26	S27	GBE1_MDI3+	I/O	GBE
GBE	I/O	GBE0_MDI1+	P27	S28	N.C.		
		N.C.	P28	S29	SERDES_0_TX+ / PCIE_D_TX+	O	SERDES / PCI-e
GBE	I/O	GBE0_MDI0-	P29	S30	SERDES_0_TX- / PCIE_D_TX-	O	SERDES / PCI-e
GBE	I/O	GBE0_MDI0+	P30	S31	GBE1_LINK_ACT#	O	GBE
		N.C.	P31	S32	SERDES_0_RX+ / PCIE_D_RX+	I	SERDES / PCI-e
		GND	P32	S33	SERDES_0_RX- / PCIE_D_RX-	I	SERDES / PCI-e
SDIO_CARD	I	SDIO_WP	P33	S34	GND		
SDIO_CARD	I/O	SDIO_CMD	P34	S35	USB4+	I/O	USB
SDIO_CARD	I	SDIO_CD#	P35	S36	USB4-	I/O	USB
SDIO_CARD	O	SDIO_CK	P36	S37	N.C.		
SDIO_CARD	O	SDIO_PWR_EN	P37	S38	AUDIO_MCK	O	AUDIO
		GND	P38	S39	I2S0_LRCK	I/O	AUDIO
SDIO_CARD	I/O	SDIO_D0	P39	S40	I2S0_SDOUT	O	AUDIO
SDIO_CARD	I/O	SDIO_D1	P40	S41	I2S0_SDIN	I	AUDIO
SDIO_CARD	I/O	SDIO_D2	P41	S42	I2S0_CK	I/O	AUDIO
SDIO_CARD	I/O	SDIO_D3	P42	S43	ESPI_ALERT0#	I	ESPI INTERFACE
SPI 0 INTERFACE	O	SPI0_CS0#	P43	S44	ESPI_ALERT1#	I	ESPI INTERFACE

SPI 0 INTERFACE	O	SPI0_CK	P44	S45	MDIO_CLK	O	SERDES
SPI 0 INTERFACE	I	SPI0_DIN	P45	S46	MDIO_DAT	I/O	SERDES
SPI 0 INTERFACE	O	SPI0_DO	P46	S47	GND		
		GND	P47	S48	I2C_GP_CK	I/O	I2C
SATA	O	SATA_TX+	P48	S49	I2C_GP_DAT	I/O	I2C
SATA	O	SATA_TX-	P49	S50	HDA_SYNC	I/O	HD AUDIO
		GND	P50	S51	HDA_SDO	O	HD AUDIO
SATA	I	SATA_RX+	P51	S52	HDA_SDI	I	HD AUDIO
SATA	I	SATA_RX-	P52	S53	HDA_CK	O	HD AUDIO
		GND	P53	S54	SATA_ACT#	O	SATA
SPI 1 / eSPI INTERFACE	O	SPI1_CS0#/ESPI_CS0#	P54	S55	USB5_EN_OC#	I/O	USB
SPI 1 / eSPI INTERFACE		SPI1_CS1#/ESPI_CS1#	P55	S56	ESPI_IO_2	I/O	eSPI INTERFACE
SPI 1 / eSPI INTERFACE	O	SPI1_CK / ESPI_CK	P56	S57	ESPI_IO_3	I/O	eSPI INTERFACE
SPI 1 / eSPI INTERFACE	I/O	SPI1_DIN / ESPI_IO_1	P57	S58	ESPI_RESET#	O	eSPI INTERFACE
SPI 1 / eSPI INTERFACE	I/O	SPI1_DO / ESPI_IO_0	P58	S59	USB5+	I/O	USB
		GND	P59	S60	USB5-	I/O	USB
USB	I/O	USB0+	P60	S61	GND		
USB	I/O	USB0-	P61	S62	USB3_SSTX+	O	USB
USB	I/O	USB0_EN_OC#	P62	S63	USB3_SSTX-	O	USB
		N.C.	P63	S64	GND		
		N.C.	P64	S65	USB3_SSRX+	I	USB
USB	I/O	USB1+	P65	S66	USB3_SSRX-	I	USB
USB	I/O	USB1-	P66	S67	GND		
USB	I/O	USB1_EN_OC#	P67	S68	USB3+	I/O	USB
		GND	P68	S69	USB3-	I/O	USB
USB	I/O	USB2+	P69	S70	GND		
USB	I/O	USB2-	P70	S71	USB2_SSTX+	O	USB
USB	I/O	USB2_EN_OC#	P71	S72	USB2_SSTX-	O	USB
FUSA	I/O	SPIM_MOSI	P72	S73	GND		
FUSA	I/O	THERMTRIP	P73	S74	USB2_SSRX+	I	USB

USB	I/O	USB3_EN_OC#	P74	S75	USB2_SSRX-	I	USB
PCI_e	O	PCIE_A_RST#	P75	S76	PCIE_B_RST#	O	PCI-e
USB	I/O	USB4_EN_OC#	P76	S77	PCIE_C_RST#	O	PCI-e
PCI-e	I	PCIE_B_CLKREQ#	P77	S78	PCIE_C_RX+	I	PCI-e
PCI-e	I	PCIE_A_CLKREQ#	P78	S79	PCIE_C_RX-	I	PCI-e
		GND	P79	S80	GND		PCI-e
PCI-e	O	PCIE_C_REFCK+	P80	S81	PCIE_C_TX+	O	PCI-e
PCI-e	O	PCIE_C_REFCK-	P81	S82	PCIE_C_TX-	O	PCI-e
		GND	P82	S83	GND		
PCI-e	O	PCIE_A_REFCK+	P83	S84	PCIE_B_REFCK+	O	PCI-e
PCI-e	O	PCIE_A_REFCK-	P84	S85	PCIE_B_REFCK-	O	PCI-e
		GND	P85	S86	GND		
PCI-e	I	PCIE_A_RX+	P86	S87	PCIE_B_RX+	I	PCI-e
PCI-e	I	PCIE_A_RX-	P87	S88	PCIE_B_RX-	I	PCI-e
		GND	P88	S89	GND		
PCI-e	O	PCIE_A_TX+	P89	S90	PCIE_B_TX+	O	PCI-e
PCI-e	O	PCIE_A_TX-	P90	S91	PCIE_B_TX-	O	PCI-e
		GND	P91	S92	GND		
DP++ INTERFACE #1	O	DP1_LANE0+	P92	S93	DP0_LANE0+	O	DP++ INTERFACE #0
DP++ INTERFACE #1	O	DP1_LANE0-	P93	S94	DP0_LANE0-	O	DP++ INTERFACE #0
		GND	P94	S95	DP0_AUX_SEL	I	DP++ INTERFACE #0
DP++ INTERFACE #1	O	DP1_LANE1+	P95	S96	DP0_LANE1+	O	DP++ INTERFACE #0
DP++ INTERFACE #1	O	DP1_LANE1-	P96	S97	DP0_LANE1-	O	DP++ INTERFACE #0
		GND	P97	S98	DP0_HPD	I	DP++ INTERFACE #0
DP++ INTERFACE #1	O	DP1_LANE2+	P98	S99	DP0_LANE2+	O	DP++ INTERFACE #0
DP++ INTERFACE #1	O	DP1_LANE2-	P99	S100	DP0_LANE2-	O	DP++ INTERFACE #0
		GND	P100	S101	GND		
DP++ INTERFACE #1	O	DP1_LANE3+	P101	S102	DP0_LANE3+	O	DP++ INTERFACE #0
DP++ INTERFACE #1	O	DP1_LANE3-	P102	S103	DP0_LANE3-	O	DP++ INTERFACE #0
		GND	P103	S104	N.C.		

DP++ INTERFACE #1	I	DP1_HPD	P104	S105	DP0_AUX+	I/O	DP++ INTERFACE #0
DP++ INTERFACE #1	I/O	DP1_AUX+	P105	S106	DP0_AUX-	I/O	DP++ INTERFACE #0
DP++ INTERFACE #1	I/O	DP1_AUX-	P106	S107	LCD1_BKLT_EN	O	LCD_SUPPORT
DP++ INTERFACE #1	I	DP1_AUX_SEL	P107	S108	LVDS1_CK+	O	PRIMARY_DISPLAY
GPIO / FUSA	I/O	GPIO0 / OKNOK0	P108	S109	LVDS1_CK-	O	PRIMARY_DISPLAY
GPIO / FUSA	I/O	GPIO1 / OKNOK1	P109	S110	GND		
GPIO / FUSA	I/O	GPIO2 / ALERT#	P110	S111	LVDS1_0+	O	PRIMARY_DISPLAY
GPIO / FUSA	I/O	GPIO3 / SPIS_CS#	P111	S112	LVDS1_0-	O	PRIMARY_DISPLAY
GPIO / FUSA	I/O	GPIO4 / SPIS_SCLK	P112	S113	N.C.		
GPIO / FUSA	I/O	GPIO5 / SPIS_MISO	P113	S114	LVDS1_1+	O	PRIMARY_DISPLAY
GPIO / FUSA	I/O	GPIO6 / SPIS_MOSI	P114	S115	LVDS1_1-	O	PRIMARY_DISPLAY
GPIO / FUSA	I/O	GPIO7 / CHXPMIC_EN	P115	S116	LCD1_VDD_EN	O	LCD_SUPPORT
GPIO / FUSA	I/O	GPIO8 / CHX_RLYSWITCH	P116	S117	LVDS1_2+	O	PRIMARY_DISPLAY
GPIO / FUSA	I/O	GPIO9 / CHXOKNOX0	P117	S118	LVDS1_2-	O	PRIMARY_DISPLAY
GPIO / FUSA	I/O	GPIO10 / CHXOKNOK1	P118	S119	GND		
GPIO / FUSA	I/O	GPIO11 / SPIM_CS#	P119	S120	LVDS1_3+	O	PRIMARY_DISPLAY
		GND	P120	S121	LVDS1_3-	O	PRIMARY_DISPLAY
MANAGEMENT	I/O	I2C_PM_CK	P121	S122	LCD1_BKLT_PWM	O	LCD_SUPPORT
MANAGEMENT	I/O	I2C_PM_DAT	P122	S123	GPIO13 / SPIM_MISO	I/O	GPIO / FUSA
BOOT_SEL	I	BOOT_SEL0#	P123	S124	GND		
BOOT_SEL	I	BOOT_SEL1#	P124	S125	LVDS0_0+ / eDP0_TX0+	O	PRIMARY_DISPLAY
BOOT_SEL	I	BOOT_SEL2#	P125	S126	LVDS0_0- / eDP0_TX0-	O	PRIMARY_DISPLAY
MANAGEMENT	O	RESET_OUT#	P126	S127	LCD0_BKLT_EN	O	LCD_SUPPORT
MANAGEMENT	I	RESET_IN#	P127	S128	LVDS0_1+ / eDP0_TX1+	O	PRIMARY_DISPLAY
MANAGEMENT	I	POWER_BTN#	P128	S129	LVDS0_1- / eDP0_TX1+	O	PRIMARY_DISPLAY
ASYNC_SERIAL	O	SER0_TX	P129	S130	GND		
ASYNC_SERIAL	I	SER0_RX	P130	S131	LVDS0_2+ / eDP0_TX2+	O	PRIMARY_DISPLAY
ASYNC_SERIAL	O	SER0_RTS#	P131	S132	LVDS0_2- / eDP0_TX2-	O	PRIMARY_DISPLAY
ASYNC_SERIAL	I	SER0_CTS#	P132	S133	LCD0_VDD_EN	O	LCD_SUPPORT
		GND	P133	S134	LVDS0_CK+ / eDP0_AUX+	O	PRIMARY_DISPLAY

ASYNC_SERIAL	O	SER1_TX	P134	S135	LVDS0_CK- / eDP0_AUX-	O	PRIMARY_DISPLAY
ASYNC_SERIAL	I	SER1_RX	P135	S136	GND		
ASYNC_SERIAL	O	SER2_TX	P136	S137	LVDS0_3+ / eDP0_TX3+	O	PRIMARY_DISPLAY
ASYNC_SERIAL	I	SER2_RX	P137	S138	LVDS0_3- / eDP0_TX3-	O	PRIMARY_DISPLAY
ASYNC_SERIAL	O	SER2_RTS#	P138	S139	I2C_LCD_CK	O	LCD_SUPPORT
ASYNC_SERIAL	I	SER2_CTS#	P139	S140	I2C_LCD_DAT	I/O	LCD_SUPPORT
ASYNC_SERIAL	O	SER3_TX	P140	S141	LCD0_BKLT_PWM	O	LCD_SUPPORT
ASYNC_SERIAL	I	SER3_RX	P141	S142	GPIO12 / SPIM_SCLK	I/O	GPIO / FUSA
		GND	P142	S143	GND		
CAN	O	CAN0_TX	P143	S144	eDP0_HPD	I	PRIMARY_DISPLAY
CAN	I	CAN0_RX	P144	S145	WDT_TIME_OUT#	O	WATCHDOG
		N.C.	P145	S146	PCIE_WAKE#	I	PCI_e
		N.C.	P146	S147	VDD_RTC		
		VDD_IN	P147	S148	LID#	I	MANAGEMENT
		VDD_IN	P148	S149	SLEEP#	I	MANAGEMENT
		VDD_IN	P149	S150	VIN_PWR_BAD#	I	MANAGEMENT
		VDD_IN	P150	S151	CHARGING#	I	MANAGEMENT
		VDD_IN	P151	S152	CHARGER_PRSNT#	I	MANAGEMENT
		VDD_IN	P152	S153	CARRIER_STBY#	O	MANAGEMENT
		VDD_IN	P153	S154	CARRIER_PWR_ON	O	MANAGEMENT
		VDD_IN	P154	S155	FORCE_RECOV#	I	BOOT_SEL
		VDD_IN	P155	S156	BATLOW#	I	MANAGEMENT
		VDD_IN	P156	S157	TEST#	I	MANAGEMENT
				S158	GND		

3.2.1.1 LCD Display Support Signals

The Intel® family of SOCs formerly coded as Elkhart Lake offers signal for direct driving of a panel and its display's backlight: enabling signals for panel (LCD0_VDD_EN) and backlight (LCD0_BKLT_EN), Backlight Brightness Control signal (LCD0_BKLT_PWM). These signals have an electrical of +1.8V_RUN, so they will be adapted/level shifted by the carrier board for external use.

There are also the signals necessary for driving I2C Data and Clock lines of LCD EDID EEPROM.

The panel control signals are:

LCD0_VDD_EN: Panel #0 Panel enable signal. Active high signal, +1.8V_RUN electrical level Output.

LCD0_BKLT_EN: Panel #0 Panel Backlight Enable signal. It can be used to turn On/Off the backlight's lamps of a connected LVDS display. Active high signal, +1.8V_RUN electrical level Output.

LCD0_BKLT_PWM: This signal can be used to adjust the Panel #0 backlight brightness in displays supporting Pulse Width Modulated (PWM) regulations.
+1.8V_RUN electrical level Output.

I2C_LCD_DAT: LCD I2C Data. This signal is used to read the LCD display EDID EEPROM. +1.8V_RUN electrical level with a 2.2kΩ pull-up resistor.

I2C_LCD_CLK: LCD I2C Clock: This signal is used to read the LCD display EDID EEPROM. +1.8V_RUN electrical level with a 2.2kΩ pull-up resistor.

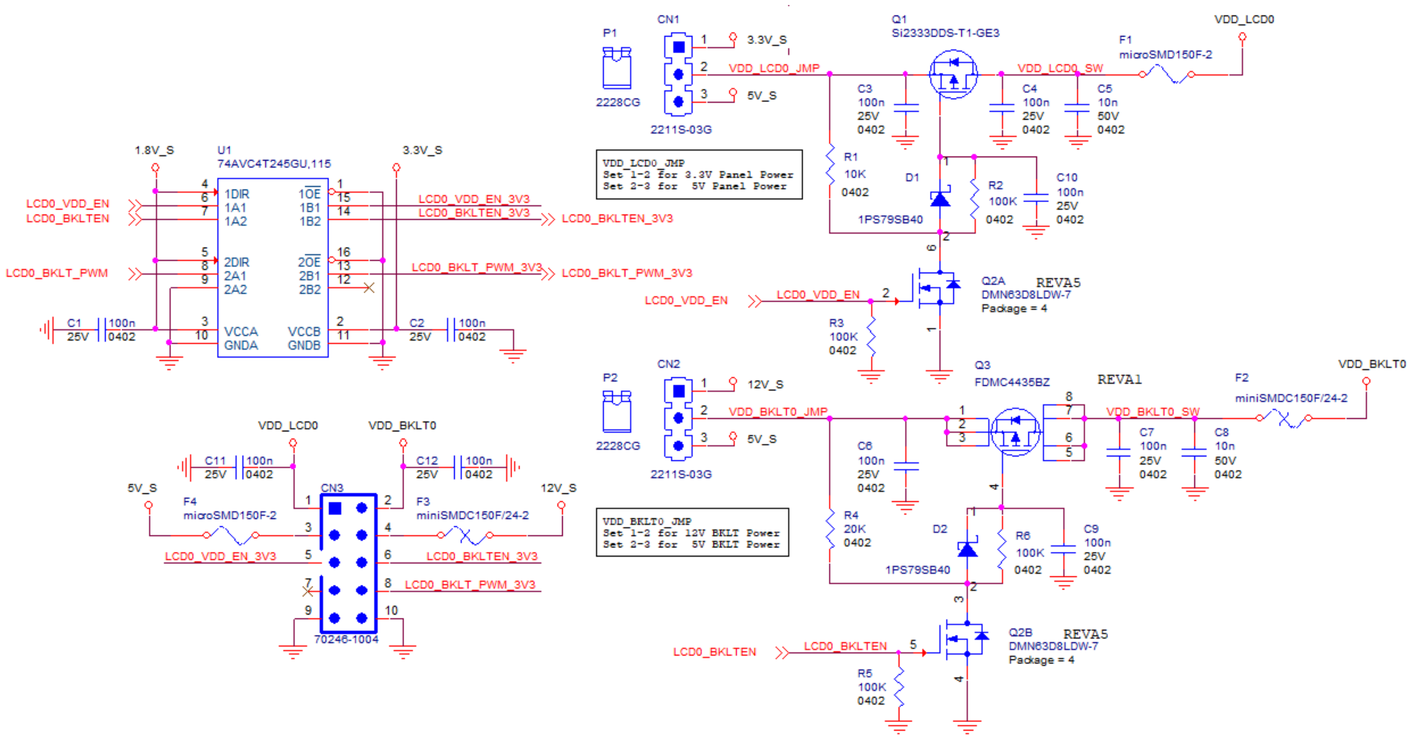
Please refer to the following schematics as an example of implementation for LCD and backlight support signals driving connection + voltage level shifters on the carrier board.

!

All schematics (henceforth also referred to as material) contained in this manual are provided by SECO S.p.A. for the sole purpose of supporting the customers' internal development activities.

The schematics are provided "AS IS". SECO makes no representation regarding the suitability of this material for any purpose or activity and disclaims all warranties and conditions with regard to said material, including but not limited to, all expressed or implied warranties and conditions of merchantability, suitability for a specific purpose, title and non-infringement of any third party intellectual property rights.

The customer acknowledges and agrees to the conditions set forth that these schematics are provided only as an example and that he will conduct an independent analysis and exercise judgment in the use of any and all material. SECO declines all and any liability for use of this or any other material in the customers' product design



3.2.1.2 eDP / Dual Channel LVDS (factory alternatives)

The Intel® family of SOCs formerly coded as Elkhart Lake offers a wide range of single and multi-purpose Digital Display Interfaces.

THE MODULE offers one embedded Display Port (eDP) interface or Dual Channel LVDS (factory alternatives), two multimode display ports (DP++) or one multimode display port (DP++) and one HDMI.

The LVDS interface, which is frequently used in many application fields, is not directly supported by the SOC. For this reason, considering that LVDS dual channel interfaces can be factory alternative on the same pins with eDP interface, on the module can be implemented an eDP to LVDS bridge (NXP PTN3460), which allow the implementation of a Dual Channel LVDS, with a maximum supported resolution of 1920x1200 @ 60Hz (dual channel mode). Such an interface is derived from the SOCs' dedicated eDP Interface.

! Please remember that LVDS interface is not native for the Intel® family of SOCs formerly coded as Elkhart Lake, it is derived from an optional eDP-to-LVDS bridge. Depending on the factory option purchased, on the same pins it is possible to have available LVDS or eDP interface. Please take care of specifying if it is necessary LVDS interface or eDP, before placing an order of this product.

ONLY ONE set of signals from the following two sets are present, dependent on the factory board configuration.

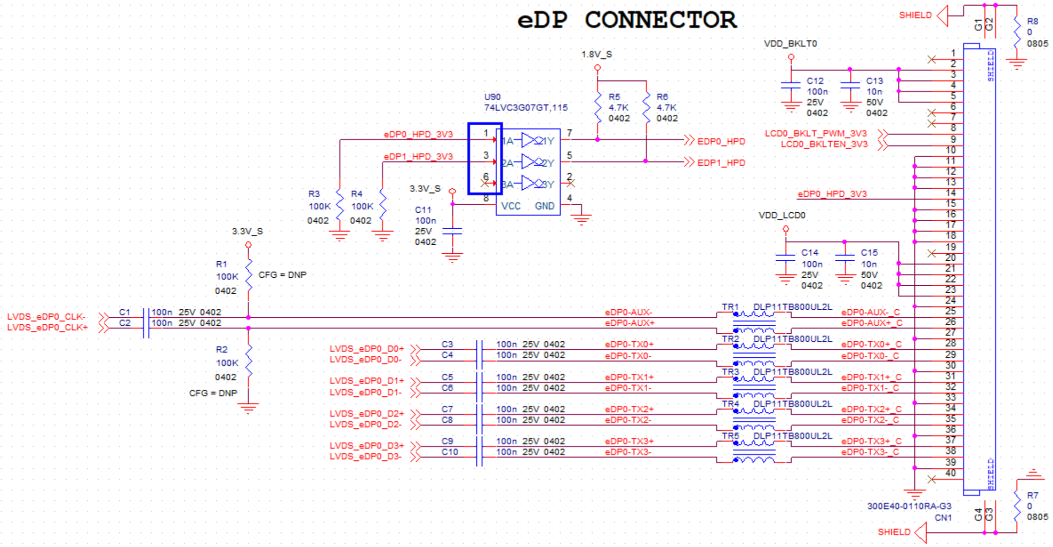
EITHER the signals for Channel #0 are LVDS:

LVDS0_0+/LVDS0_0-: LVDS Channel #0 differential data pair #0.
LVDS0_1+/LVDS0_1-: LVDS Channel #0 differential data pair #1.
LVDS0_2+/LVDS0_2-: LVDS Channel #0 differential data pair #2.
LVDS0_3+/LVDS0_3-: LVDS Channel #0 differential data pair #3.
LVDS0_CK+/LVDS0_CK-: LVDS Channel #0 differential Clock.

OR the signals for Channel #0 are eDP:

eDP0_TX0+/ eDP0_TX0-: eDP Channel #0 differential data pair #0.
eDP0_TX1+/ eDP0_TX1-: eDP Channel #0 differential data pair #1.
eDP0_TX2+/ eDP0_TX2-: eDP Channel #0 differential data pair #2.
eDP0_TX3+/ eDP0_TX3-: eDP Channel #0 differential data pair #3.
eDP0_AUX+/ eDP0_AUX-: eDP Channel #0 differential Clock.
eDP0_HPD: Hot Plug Detect, Active high Input signal of +1.8V_RUN electrical level from carrier board. 1MΩ pull-down resistor is placed on module for this signal.

Please refer to the following schematics as an example of connection of eDP interface on the carrier board. Hot Plug Detect signal must be buffered to prevent back feeding of power from the display to the module as well as level translation.



The signals for Channel #1 are LVDS, when this interface is selected in factory board configuration, otherwise these pins will be not connected.

LVDS1_1+ / LVDS1_0- : LVDS Channel #1 differential data pair #0

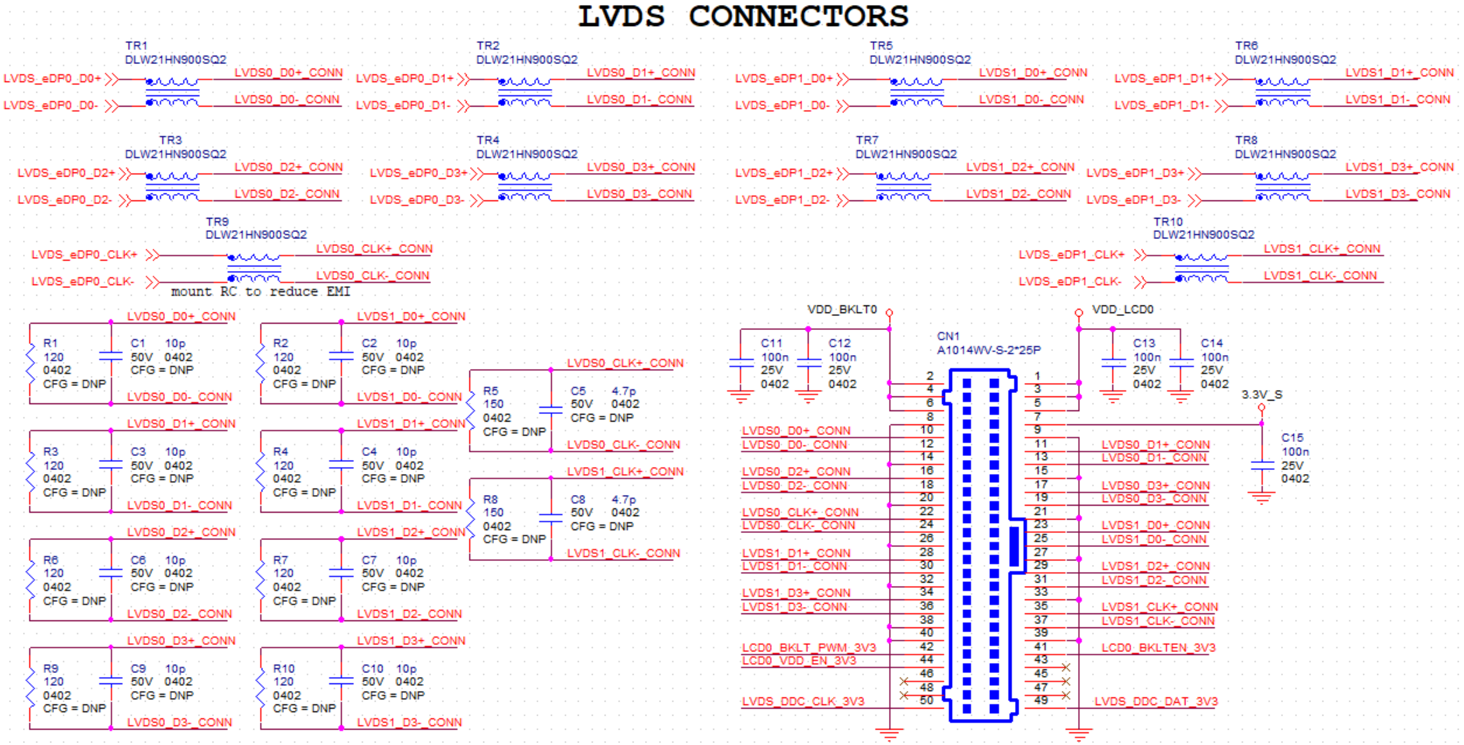
LVDS1_1+/ LVDS1_1-: LVDS Channel #1 differential data pair #1

LVDS1_2+/LVDS1_2-: LVDS Channel #1 differential data pair #2

LVDS1_3+/ LVDS1_3-: LVDS Channel #1 differential data pair #3

LVDS1_CK+/ LVDS1_CK-: LVDS Channel #1 differential Clock

Please refer to the following schematics as an example of connection of dual channel LVDS interface on the carrier board, with EMI filtering section included.



3.2.1.3 HDMI / DP++ (factory alternatives) interface signals

As described in the previous paragraph, the Intel® family of SOCs formerly coded as Elkhart Lake offers, as secondary display interface, a native multimode Digital Display Interface, configurable as a factory alternative to work as a multimode Display Port (DP++) with a resolution up to 4096 x 2160 @60Hz or DC coupled HDMI signals for the implementation on the carrier board of a decoupling circuit for HDMI v1.4 with a resolution up to 3840 x 2160 @30Hz or a retimer circuit for HDMI 2.0 for color depth up to 16 bit.

EITHER the signals for the Channel are HDMI:

HDMI_D0+/HDMI_D0-: HDMI Output Differential Pair #0

HDMI_D1+/HDMI_D1-: HDMI Output Differential Pair #1

HDMI_D2+/HDMI_D2-: HDMI Output Differential Pair #2

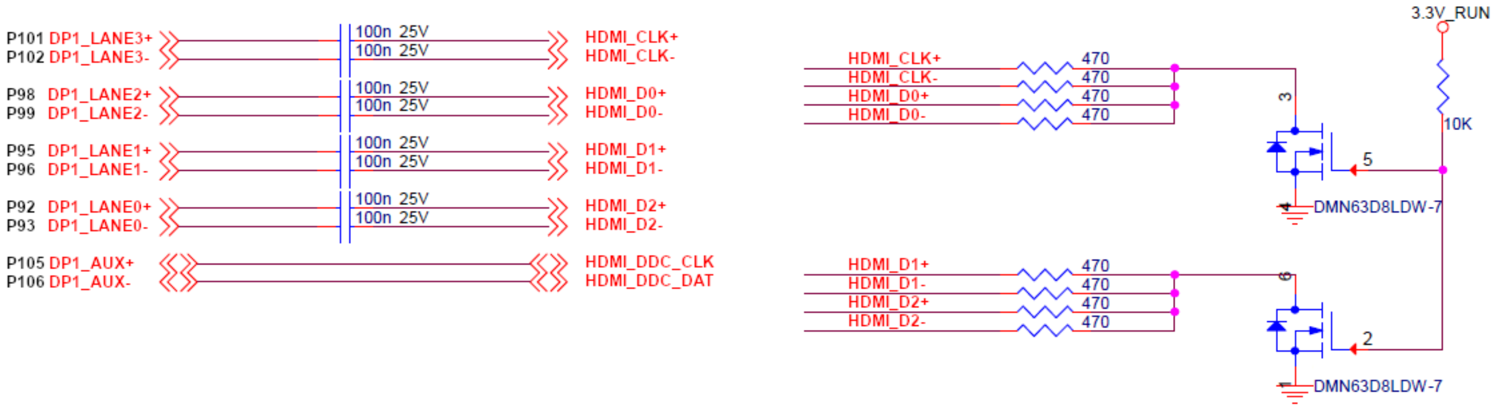
HDMI_CK+/HDMI_CK-: HDMI Differential Clock

HDMI_HPD: Hot Plug Detect, Active high Input signal of +1.8V_RUN electrical level from carrier board. 1MΩ pull-down resistor is placed on module for this signal.

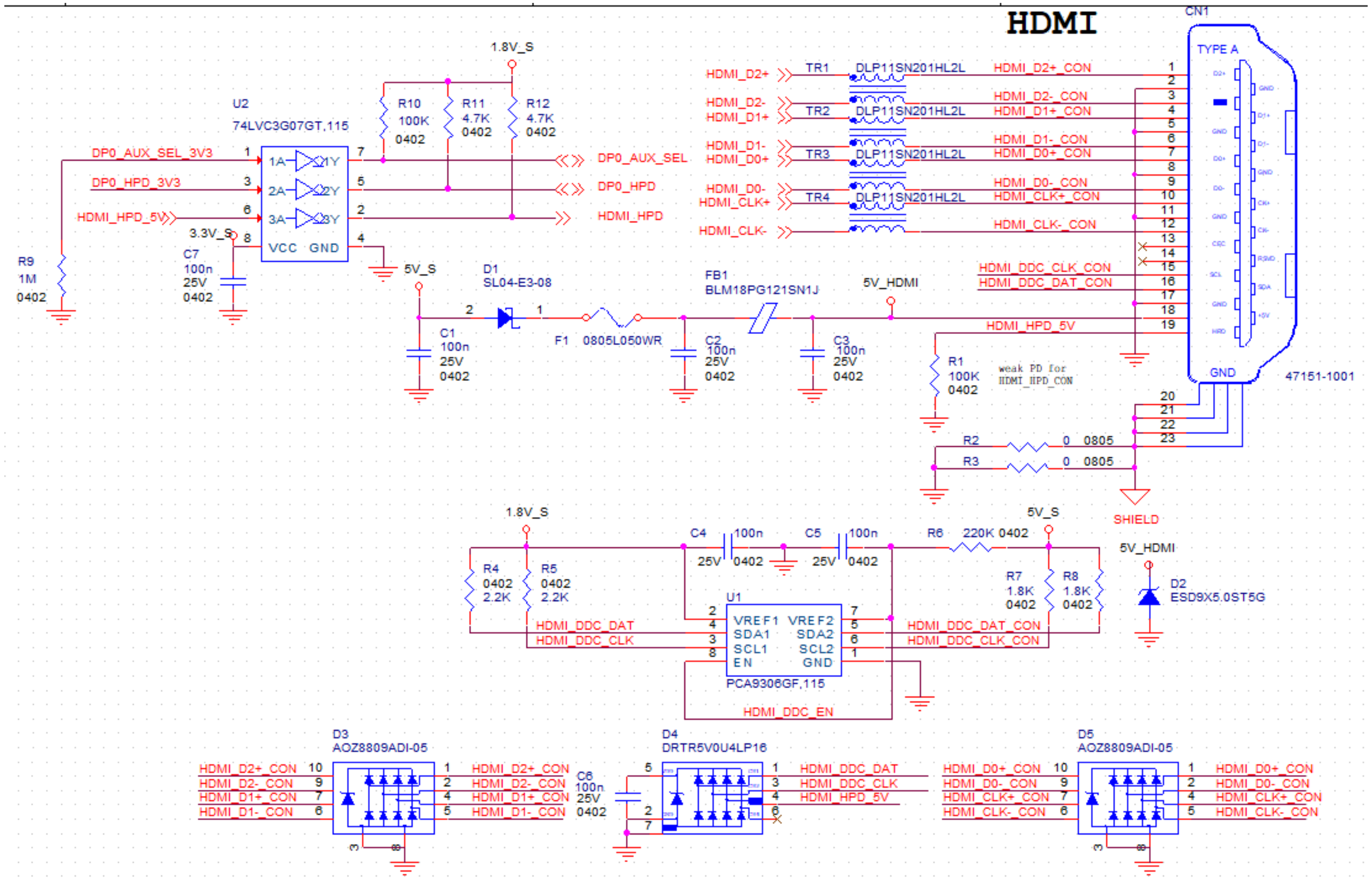
HDMI_CTRL_CK: DDC Clock line for HDMI panel. Bidirectional signal, +1.8V_RUN electrical level with a 100kΩ pull-up resistor

HDMI_CTRL_DAT: DDC Data line for HDMI panel. Bidirectional signal, +1.8V_RUN electrical level with a 100kΩ pull-up resistor

Please refer to the following schematics as an implementation example of the decoupling circuit for HDMI 1.4 compliance. For implementation of a retimer circuit for HDMI 2.0 compliance please refer to the TI SN75DP159 datasheet for reference designs.



Please refer to the following schematics as an example of connection of HDMI interface on the carrier board, with Voltage clamping diodes highly recommended on all signal lines for ESD suppression, as well as common mode choke inductors for EMI purpose. Voltage level shifters are necessary on Control data/Clock signals, as well as for Hot Plug Detect signal.



OR the signals for the Channel are DP++:

DP1_LANE0+/ DP1_LANE0-: DP Channel #1 Output Differential Pair #0

DP1_LANE1+/ DP1_LANE1-: DP Channel #1 Output Differential Pair #1

DP1_LANE2+/ DP1_LANE2-: DP Channel #1 Output Differential Pair #2

DP1_LANE3+/ DP1_LANE3-: DP Channel #1 Output Differential Pair #3

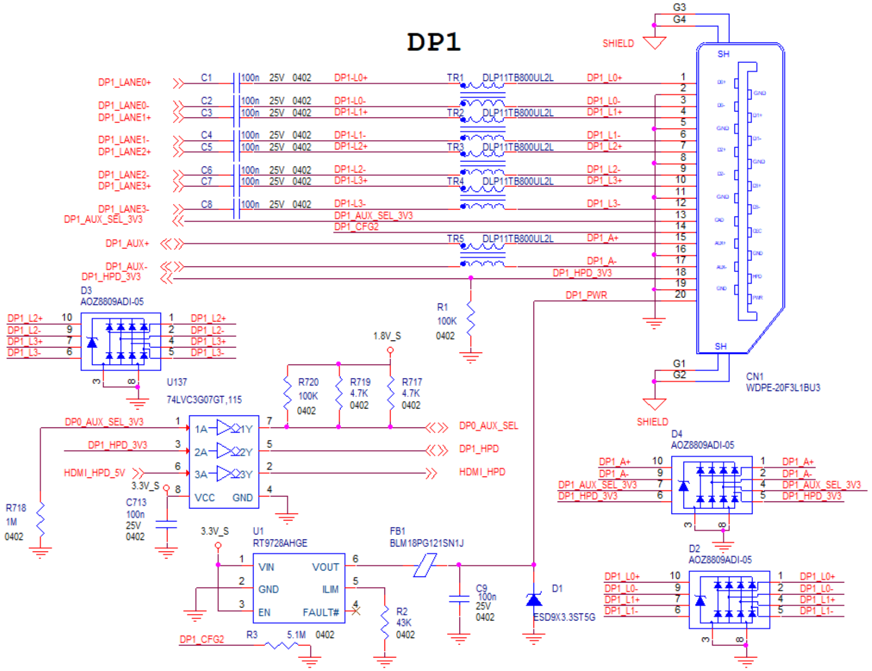
DP1_AUX+: DDC Clock line for DP Channel #1. Bidirectional signal, +3.3V_RUN electrical level with a 100kΩ pull-up resistor

DP1_AUX-: DDC Data line for DP Channel #1. Bidirectional signal, +3.3V_RUN electrical level with a 100kΩ pull-up resistor

DP1_HPD: Hot Plug Detect, Active high Input signal of +1.8V_RUN electrical level from carrier board. 1MΩ pull-down resistor is placed on module for this signal.

DP1_AUX_SEL: Select input signal to switch between I2C Clock/Data for HDMI (high level) and Display Port Auxiliary Channel for DP/HDMI (low level). 1MΩ pull-down resistor is placed on module for this signal.

Please refer to the following schematics as an example of connection of DP interface on the carrier board, with Voltage clamping diodes highly recommended on all signal lines for ESD suppression. Hot Plug Detect signal must be buffered to prevent back feeding of power from the display to the module as well as level translation. Switch with settable current limit on power lines are recommended.



3.2.1.4 DP++ interface signals

As described in the previous paragraph, the Intel® family of SOCs formerly coded as Elkhart Lake offers a native multimode Display Port (DP) interface, with a resolution up to 4096 x 2160 @60Hz

The signals related to DP++ are as follows:

DP0_LANE0+/ DP0_LANE0-: DP Channel #0 differential data pair #0.

DP0_LANE1+/ DP0_LANE1-: DP Channel #0 differential data pair #1.

DP0_LANE2+/ DP0_LANE2-: DP Channel #0 differential data pair #2.

DP0_LANE3+/ DP0_LANE3-: DP Channel #0 differential data pair #3.

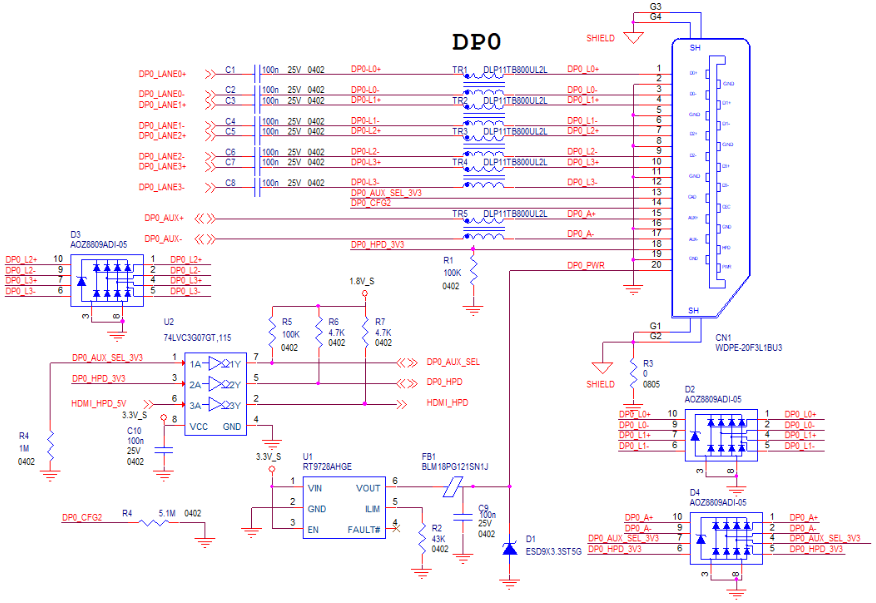
DP0_HPD: Hot Plug Detect, Active high Input signal of +1.8V_RUN electrical level from carrier board. 1MΩ pull-down resistor is placed on module for this signal.

DP0_AUX+: DDC Clock line for DP Channel #0. Bidirectional signal, +3.3V_RUN electrical level with a 100kΩ pull-up resistor

DP0_AUX-: DDC Data line for DP Channel #0. Bidirectional signal, +3.3V_RUN electrical level with a 100kΩ pull-up resistor

DP0_AUX_SEL: Select input signal to switch between I2C Clock/Data for HDMI (high level) and Display Port Auxiliary Channel for DP/HDMI (low level). 1MΩ pull-down resistor is placed on module for this signal.

Please refer to the following schematics as an example of connection of DP interface on the carrier board, with Voltage clamping diodes highly recommended on all signal lines for ESD suppression. Hot Plug Detect signal must be buffered to prevent back feeding of power from the display to the module as well as level translation. Switch with settable current limit on power lines are recommended.



3.2.1.5 SATA interface signals

The Intel® family of SOCs formerly coded as Elkhart Lake offers one S-ATA interface.

The interface is Gen3 compliant, with support of 1.5Gbps, 3.0 Gbps and 6.0 Gbps data rates

Here following the signals related to SATA interface:

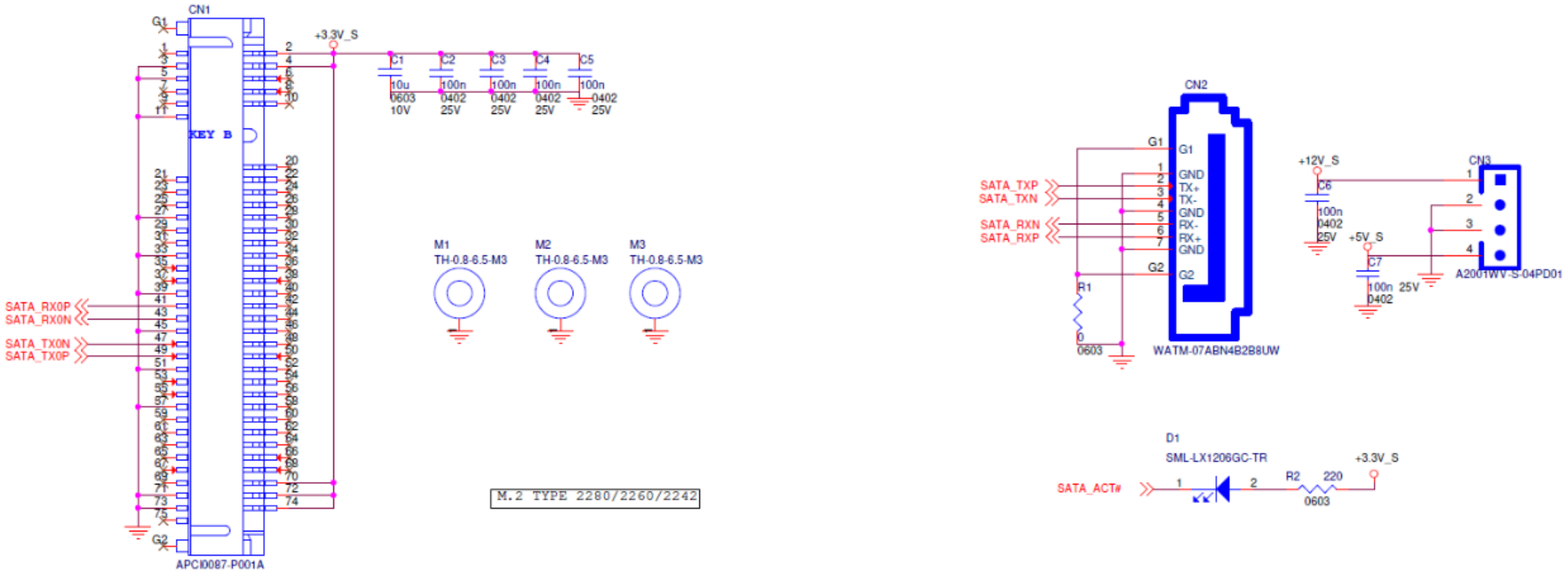
SATA_TX+/SATA_TX-: Serial ATA Channel #1 Transmit differential pair

SATA_RX+/SATA_RX-: Serial ATA Channel #1 Receive differential pair

SATA_ACT#: Serial ATA Activity Led. Active low output signal at +3.3V_RUN voltage

10nF AC series decoupling capacitors are placed on each line of SATA differential pairs.

On the carrier board, these signals can be carried out directly to a SATA M 7p connector or switched for an M.2 SSD Slot, which allow plugging M.2 Socket 2 Key B Solid State Drives. Please refer to the following schematics as an example of connection of SATA interface on the carrier board to selected connector.



3.2.1.6 SDI/O interface signals

The Intel® family of SOCs formerly coded as Elkhart Lake offers one SD Card controller, able to support SD Card 3.0 interface.

Such an SD controller complies with SD Host Controller Standard Specification version 3.01 and only supports devices for data storage.

The SD port is externally accessible through the SD Card Slot connector, can work in 1-bit and 4-bit mode operation with data rate up to 104MB/s.

The signals related to SDIO are as follows:

SDIO_WP: Write Protect input, electrical level +3.3V_RUN with 10kΩ pull-up resistor. It is used to communicate the status of Write Protect switch of the external SD card. Since microSD cards don't manage this signal, it is important that, when designing carrier boards with microSD slots, this signal must be tied to GND, otherwise the OS will always consider the card as protected from writing.

SDIO_CMD: Command/Response line. Bidirectional signal, electrical level +3.3V_RUN, used to send command from Host (Intel processor) to the connected card, and to send the response from the card to the Host.

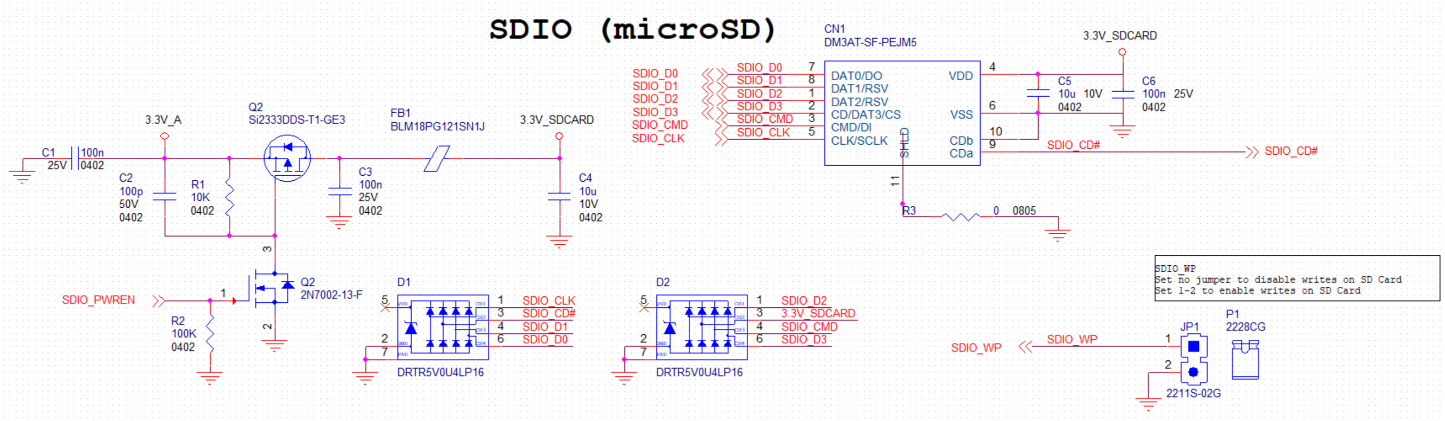
SDIO_CD#: Card Detect Input. Active Low Signal, electrical level +3.3V_RUN with 10kΩ pull-up resistor. This signal must be externally pulled low to signal that a SDIO/MMC Card is present.

SDIO_CK: Clock Line (output), 50 MHz maximum frequency for SD/SDIO High Speed Mode.

SDIO_PWR_EN: SDIO Power Enable output, active high signal, electrical level +3.3V_RUN. It is used to enable the power line supplying SD/SDIO/MMC devices.

SDIO_[D0÷D3]: SD Card data bus. SDIO_D0 signal is used for all communication modes. SDIO_[D1÷D3] signals are required for 4-bit communication mode.

Please refer to the following schematics as an example of connection of SDIO interface on the carrier board, with Voltage clamping diodes highly recommended on all signal lines for ESD suppression.



3.2.1.7 SPI interface signals

The Intel® family of SOCs formerly coded as Elkhart Lake offers also one dedicated Serial Peripheral Interface (SPI0) for boot device purpose and one general purpose Serial Peripheral Interface (SPI1) or eSPI (factory alternatives).

The signals related to SPI0 are as follows:

SPI0_CS0#: SPI channel #0 primary Chip select, active low output signal. Electrical level +1.8V_ALW

On the same bus there is a second SPI slave device (BIOS flash boot device), mounted on the module, connected to a dedicated chip select signal

SPI0_CK: SPI channel #0 Clock Output to carrier board's SPI embedded devices. Electrical level +1.8V_ALW

SPI0_DIN: SPI channel #0 Master Data Input, electrical level +1.8V_ALW

SPI0_DO: SPI channel #0 Master Data Output, electrical level +1.8V_ALW

ONLY ONE set of signals from the following two sets are present, dependent on the factory board configuration.

EITHER the signals for the SPI1 are general-purpose SPI bus:

SPI1_CS0#: SPI channel #1 primary Chip select, active low output signal. Electrical level +1.8V_ALW

SPI1_CS1#: SPI channel #1 secondary Chip select, active low output signal. Electrical level +1.8V_ALW

SPI1_CK: SPI channel #1 Clock Output to carrier board's SPI embedded devices. Electrical level +1.8V_ALW

SPI1_DIN: SPI0 channel #1 Master Data Input, electrical level +1.8V_ALW

SPI1_DO: SPI0 channel #1 Master Data Output, electrical level +1.8V_ALW

OR the signals for the SPI1 are Enhanced Serial Peripheral Interface (eSPI) bus:

ESPI_CK: ESPI Master Clock Output. Electrical level +1.8V_ALW. The reference timing signal for all the serial input and output operations

ESPI_CS0#: ESPI Master Chip Select Output #0. Electrical level +1.8V_ALW. Driven low by the processor to select the ESPI slave device on the carrier board.

ESPI_CS1#: ESPI Master Chip Select Output #1. Electrical level +1.8V_ALW. This signal must be used only in case there are two ESPI devices on the carrier board, and the first chip select signal (ESPI_CS0#) has already been used. It must not be used in case there is only one ESPI device

ESPI_IO_[0:3]: ESPI Master Data Bidirectional. Electrical level +1.8V_ALW. Data transfer between the master and slaves. In Single I/O mode, ESPI_IO_0 is the eSPI master output/eSPI slave input (MOSI) whereas ESPI_IO_1 is the eSPI master input/eSPI slave output (MISO).

ESPI_RESET#: ESPI Reset. Output. Electrical level +1.8V_ALW with 75kΩ pull-down resistor. Reset the ESPI interface for both master and slaves.

ESPI_ALERT0#: Alert signal driven by the slave ESPI slave device #0. Input. Electrical level +1.8V_ALW

ESPI_ALERT1#: Alert signal driven by the slave ESPI slave device #1. Input. Electrical level +1.8V_ALW

3.2.1.8 Audio interface signals

The Intel® family of SOCs formerly coded as Elkhart Lake supports I2S and HD audio format, thanks to native support offered by the processor to this audio codec standard.

Here are following the signals related to I2S Audio interface:

AUDIO_MCK: Master clock output to Audio codec. Output from the module to the Carrier board, electrical level +1.8V_RUN

I2S0_LRCK: Left& Right audio interface #0 synchronization clock. Bi-Directional between the module to the Carrier board, electrical level +1.8V_RUN

I2S0_SDOUT: Digital audio interface #0 Output. Output from the module to the Carrier board, electrical level +1.8V_RUN

I2S0_SDIN: Digital audio interface #0 Input. Input from the module to the Carrier board, electrical level +1.8V_RUN

I2S0_CK: Digital audio interface #0 clock. Bi-Directional between the module to the Carrier board, electrical level +1.8V_RUN

All these signals can be connected, on the Carrier Board, to an I2S Audio Codec. Please refer to the chosen Codec's Reference Design Guide for correct implementation of audio section on the carrier board.

Here are following the signals related to HD Audio interface:

HDA_SYNC: Synchronization clock. Bi-Directional between the module to the Carrier board, electrical level +1.8V_RUN

HDA_SDO: Digital audio Output. Output from the module to the Carrier board, electrical level +1.8V_RUN

HDA_SDI: Digital audio Input. Input from the module to the Carrier board, electrical level +1.8V_RUN

HDA_CK: Digital audio clock. Bi-Directional between the module to the Carrier board, electrical level +1.8V_RUN

HDA_RST#: Digital Audio Reset. This signal is multiplexed with GPIO4. This pin has to be defined via BIOS so that GPIO4/HDA_RST# is in HDA_RST# modality.

All these signals have to be connected, on the Carrier Board, to an HD Audio Codec. Please refer to the chosen Codec's Reference Design Guide for correct implementation of audio section on the carrier board.

3.2.1.9 I2C / SM bus Interface

The Intel® family of SOCs formerly coded as Elkhart Lake supports one general purpose I2C interface and one power management SM bus.

Here are following the signals related to general purpose I2C interface:

I2C_GP_CK: I2C General Purpose clock signal. Bi-Directional between the module to the Carrier board, electrical level +1.8V_RUN with 2.2kΩ pull-up resistor

I2C_GP_DAT: I2C General Purpose data signal. Bi-Directional between the module to the Carrier board, electrical level +1.8V_RUN with 2.2kΩ pull-up resistor

Here are following the signals related to power management SM bus:

I2C_PM_CK: SMB Power management clock signal. Bi-Directional between the module to the Carrier board, electrical level +1.8V_ALW with 2.2kΩ pull-up resistor.

This signal is managed by the Embedded controller MEC1705 from Microchip.

I2C_PM_DAT: SMB Power management data signal. Bi-Directional between the module to the Carrier board, electrical level +1.8V_ALW with 2.2kΩ pull-up resistor

This signal is managed by the Embedded controller MEC1705 from Microchip.

3.2.1.10 Asynchronous Serial Ports (UART) interface signals

The Intel® family of SOCs formerly coded as Elkhart Lake offers in its Low Power Sub System (LPSS) two high speed UART, with a maximum speed of 115,200 kb/s or 3.6864Mb/s depending on Industry standards.

In addition, two additional UART are offered and managed by the Embedded controller MEC1705 from Microchip

SER0_TX: UART #0 Interface, Serial data Transmit (output) line, 1.8V_RUN electrical level. It is managed by Microchip MEC1705 controller.

SER0_RX: UART #0 Interface, Serial data Receive (input) line, 1.8V_RUN electrical level. It is managed by Microchip MEC1705 controller.

SER0_RTS#: UART #0 Interface, Handshake signal, Request to Send (output) line, 1.8V_ RUN electrical level

SER0_CTS#: UART #0 Interface, Handshake signal, Clear to Send (Input) line, 1.8V_ RUN electrical level

SER1_TX: HS-UART #0 Interface, Serial data Transmit (output) line, 1.8V_ RUN electrical level. It is directly managed by Intel processor.

SER1_RX: HS-UART #0 Interface, Serial data Receive (input) line, 1.8V_ RUN electrical level. It is directly managed by Intel processor.

SER2_TX: UART #1 Interface, Serial data Transmit (output) line, 1.8V_ RUN electrical level. It is managed by Microchip MEC1705 controller.

SER2_RX: UART #1 Interface, Serial data Receive (input) line, 1.8V_ RUN electrical level. It is managed by Microchip MEC1705 controller.

SER2_RTS#: UART #1 Interface, Handshake signal, Request to Send (output) line, 1.8V_ RUN electrical level.

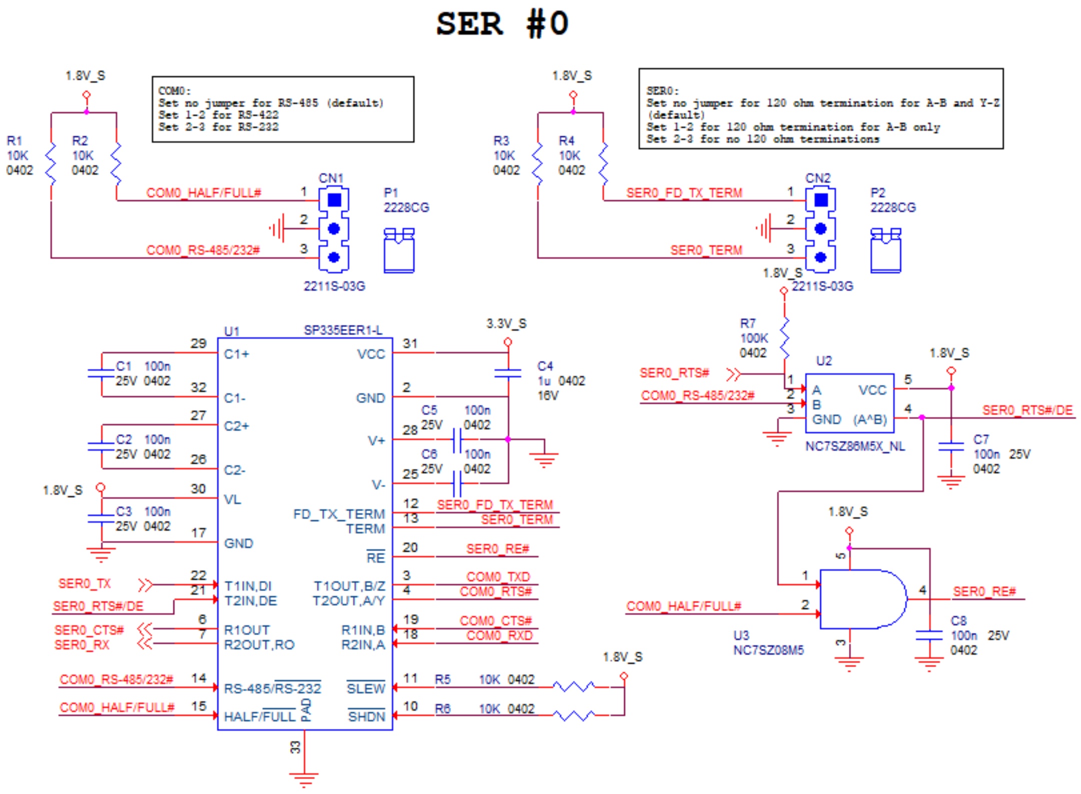
SER2_CTS#: UART #1 Interface, Handshake signal, Clear to Send (Input) line, 1.8V_ RUN electrical level.

SER3_RX: HS-UART #1 Interface, Serial data Receive (input) line, +1.8V_RUN electrical level. It is directly managed by Intel processor.

SER3_TX: HS-UART #1 Interface, Serial data Transmit (output) line, +1.8V_RUN electrical level. It is directly managed by Intel processor.

Please consider that interface is at +1.8V_ RUN electrical level; therefore, please evaluate well the typical scenario of application. If there isn't any explicit need of interfacing directly at +1.8V_ RUN level, for connection to standard serial ports commonly available (like those offered by common PCs, for example) it is mandatory to include an RS-232 transceiver on the carrier board.

In the following schematic here is an example of UART interface on the carrier board, with a multiprotocol transceiver allowing to support RS485/RS-422/RS-232 serial interfaces.



3.2.1.11 USB interface signals

The Intel® family of SOCs formerly coded as Elkhart Lake offers an xHCI USB controller, which is able to manage up to 4 Superspeed ports (i.e. USB 3.1 compliant) and up to 10 ports in USB 2.0 mode only, one of them also capable of OTG.

In THE MODULE, there are up to 6 ports in USB2.0 only and up to 2 Super Speed (SS) ports (i.e. USB 3.1 compliant).

All USB 2.0 ports are able to work in High Speed (HS), Full Speed (FS) and Low Speed (LS).

Here following the signals related to USB interfaces.

USB0+/ USB0-: Universal Serial Bus 2.0 Port #0 differential pair (directly managed by Intel processor)

USB0_EN_OC#: Power Enable and over current monitoring function. Active Low Output signal, +3.3V_ALW electrical level with a 10kΩ pull-up resistor. Refer to SMARC 2.1 Specification for over current operation information.

USB1+/ USB1-: Universal Serial Bus Port 2.0 #1 differential pair.

USB1_EN_OC#: Power Enable and over current monitoring function. Active Low Output signal, +3.3V_ALW electrical level with a 10kΩ pull-up resistor. Refer to SMARC 2.1 Specification for OC operation information.

USB2+/USB2-: Universal Serial Bus Port 2.0 #2 differential pair.

USB2_EN_OC#: Power Enable and over current monitoring function. Active Low Output signal, +3.3V_ALW electrical level with a 10kΩ pull-up resistor. Refer to SMARC 2.1 Specification for OC operation information.

USB3+/USB3-: Universal Serial Bus Port 2.0 #3 differential pair.

USB3_EN_OC#: Power Enable and over current monitoring function. Active Low Output signal, +3.3V_ALW electrical level with a 10kΩ pull-up resistor. Refer to SMARC 2.1 Specification for OC operation information.

USB4+/USB4-: Universal Serial Bus Port 2.0 #4 differential pair.

USB4_EN_OC#: Power Enable and over current monitoring function. Active Low Output signal, +3.3V_ALW electrical level with a 10kΩ pull-up resistor. Refer to SMARC 2.1 Specification for OC operation information.

USB5+/USB5-: Universal Serial Bus Port 2.0 #3 differential pair.

USB5_EN_OC#: Power Enable and over current monitoring function. Active Low Output signal, +3.3V_ALW electrical level with a 10kΩ pull-up resistor. Refer to SMARC 2.1 Specification for OC operation information.

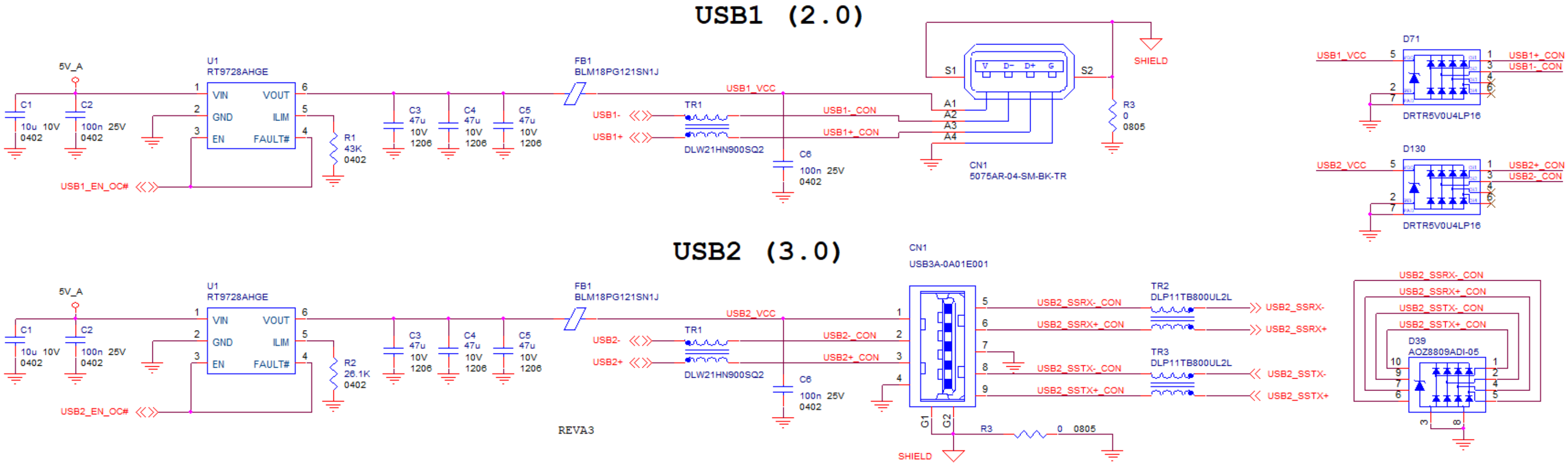
USB2_SSTX+/ USB2_SSTX-: USB 3.0 Port #1 Superspeed Transmit differential pair.

USB2_SSRX+/ USB2_SSRX-: USB 3.0 Port #1 Superspeed Receive differential pair.

USB3_SSTX+/ USB3_SSTX-: USB 3.0 Port #2 Superspeed Transmit differential pair.

USB3_SSRX+/ USB3_SSRX-: USB 3.0 Port #2 Superspeed Receive differential pair.

For EMI/ESD protection, common mode chokes on USB data lines, and clamping diodes on USB data and voltage lines, are also needed. Switch with settable current limit on power lines are recommended.



3.2.1.12 PCI Express interface signals

The module can offer externally up to four PCI Express lane, which are directly managed by the Intel® family of SOCs formerly coded as Elkhart Lake.

PCI express Gen 3.0 (8GT/s) is supported.

Here following the signals involved in PCI express management

PCIE_A_RX+/ PCIE_A_RX-: PCI Express lane #0, Receiving Input Differential pair

PCIE_A_TX+/PCIE_A_TX-: PCI Express lane #0, Transmitting Output Differential pair

PCIE_A_REFCK+/ PCIE_A_REFCK-: PCI Express Reference Clock for lane #0, Differential Pair

PCIE_A_RST#: Reset Signal that is sent from SMARC Module to a PCI-e device available on the carrier board. Active Low, +3.3V_RUN electrical level with a 100kΩ pull-down resistor. It can be used directly to drive externally a single RESET Signal. In case Reset signal is needed for multiple devices, it is recommended to provide for a buffer on the carrier board.

PCIE_A_CKREQ#: PCI Express Port A clock request signal, used from a PCI-e device to request the need for PCI Express Reference Clock. Bidirectional signal, +3.3V_RUN electrical level with a 10k pull-up resistor.

PCIE_B_RX+/ PCIE_B_RX-: PCI Express lane #1, Receiving Input Differential pair

PCIE_B_TX+/PCIE_B_TX-: PCI Express lane #1, Transmitting Output Differential pair

PCIE_B_REFCK+/ PCIE_B_REFCK-: PCI Express Reference Clock for lane #1, Differential Pair

PCIE_B_RST#: Reset Signal that is sent from SMARC Module to a PCI-e device available on the carrier board. Active Low, +3.3V_RUN electrical level with a 100kΩ pull-down resistor. It can be used directly to drive externally a single RESET Signal. In case Reset signal is needed for multiple devices, it is recommended to provide for a buffer on the carrier board. This signal is shared

PCIE_B_CKREQ#: PCI Express Port B clock request signal, used from a PCI-e device to request the need for PCI Express Reference Clock. Bidirectional signal, +3.3V_RUN electrical level with a 10k pull-up resistor.

PCIE_C_RX+/ PCIE_C_RX-: PCI Express lane #2, Receiving Input Differential pair

PCIE_C_TX+/PCIE_C_TX-: PCI Express lane #2, Transmitting Output Differential pair

PCIE_C_REFCK+/ PCIE_C_REFCK-: PCI Express Reference Clock for lane #2, Differential Pair

PCIE_C_RST#: Reset Signal that is sent from SMARC Module to a PCI-e device available on the carrier board. Active Low, +3.3V_RUN electrical level with a 100kΩ pull-down resistor. It can be used directly to drive externally a single RESET Signal. In case Reset signal is needed for multiple devices, it is recommended to provide for a buffer on the carrier board.

PCIE_D_RX+/ PCIE_D_RX-: PCI Express lane #3, Receiving Input Differential pair

PCIE_D_TX+/PCIE_D_TX-: PCI Express lane #3, Transmitting Output Differential pair

PCIE_WAKE#: PCIe wake up interrupt to host input signal. Active low, +3.3V_ALW electrical level with a 10k pull-up resistor.

In the following table are shown the possible groupings allowed of the PCI-e lanes:

<table>
<tr><th>Allowed groupings</th><th>Lane #0</th><th>Lane #1</th><th>Lane #2</th><th>Lane #3</th></tr>
<tr><td>1 PCI-e x 4 port</td><td colspan="4">√</td></tr>
<tr><td>2 PCI- e x2</td><td colspan="2">√</td><td colspan="2">√</td></tr>
<tr><td>1 PCI-e x 2 + 2 PCI-e x1</td><td colspan="2">√</td><td>√</td><td>√</td></tr>
<tr><td>4 PCI-e x1</td><td>√</td><td>√</td><td>√</td><td>√</td></tr>
</table>

Please also be aware that this grouping cannot be changed dynamically, it is a fixed feature of the BIOS.

The customer in phase of order must select what grouping to have for PCI-e lanes.

3.2.1.13 SERDES interface signal

The module can offer one optional SERDES interface, alternative to fourth PCI-e lane. The most common use for this interface is the implementation of an additional LAN port on carrier board with SGMII interface.

Here following the signals involved in SERDES management:

SERDES_0_TX+/ SERDES_0_TX-: Differential SERDES 0 Transmit Data Pair

SERDES_0_RX+/ SERDES_0_RX-: Differential SERDES 0 Receive Data Pair

MDIO_CLK: MDIO Signals to Configure Possible PHYs. +1.8V_ RUN electrical level with 2k2Ω pull-up resistor.

MDIO_DAT: MDIO Signals to Configure Possible PHYs. +1.8V_ RUN electrical level with 2k2Ω pull-up resistor.

3.2.1.14 Gigabit Ethernet signals

Gigabit Ethernet interfaces are realized on the module by using two TI Gigabit Ethernet PHY transceivers DP83867, which are interfaced to Intel processor through RGMII interface.

Here following the signals involved in Gigabit Ethernet #0 management:

GBE0_MDI0+/GBE0_MDI0-: Media Dependent Interface (MDI) Transmit/Receive differential pair

GBE0_MDI1+/GBE0_MDI1-: Media Dependent Interface (MDI) Transmit differential pair

GBE0_MDI2+/GBE0_MDI2-: Media Dependent Interface (MDI) Transmit differential pair

GBE0_MDI3+/GBE0_MDI3-: Media Dependent Interface (MDI) Transmit differential pair

GBE0_LINK_ACT#: Ethernet controller activity indicator. Active Low Output signal, +3.3V_ALW electrical level

GBE0_LINK100#: Ethernet controller 100Mbps link indicator. Active Low Output signal, +3.3V_ALW electrical level

GBE0_LINK1000#: Ethernet controller 1Gbps link indicator. Active Low Output signal, +3.3V_ALW electrical level

GBE0_SDP: Software defined pin, directly managed by TI Gigabit Ethernet PHY transceiver #0. Bidirectional signal, +3.3V_ALW electrical level.

Here following the signals involved in Gigabit Ethernet #1 management:

GBE1_MDI0+/GBE1_MDI0-: Media Dependent Interface (MDI) Transmit/Receive differential pair

GBE1_MDI1+/GBE1_MDI1-: Media Dependent Interface (MDI) Transmit differential pair

GBE1_MDI2+/GBE1_MDI2-: Media Dependent Interface (MDI) Transmit differential pair

GBE1_MDI3+/GBE1_MDI3-: Media Dependent Interface (MDI) Transmit differential pair

GBE1_LINK_ACT#: Ethernet controller activity indicator. Active Low Output signal, +3.3V_ALW electrical level

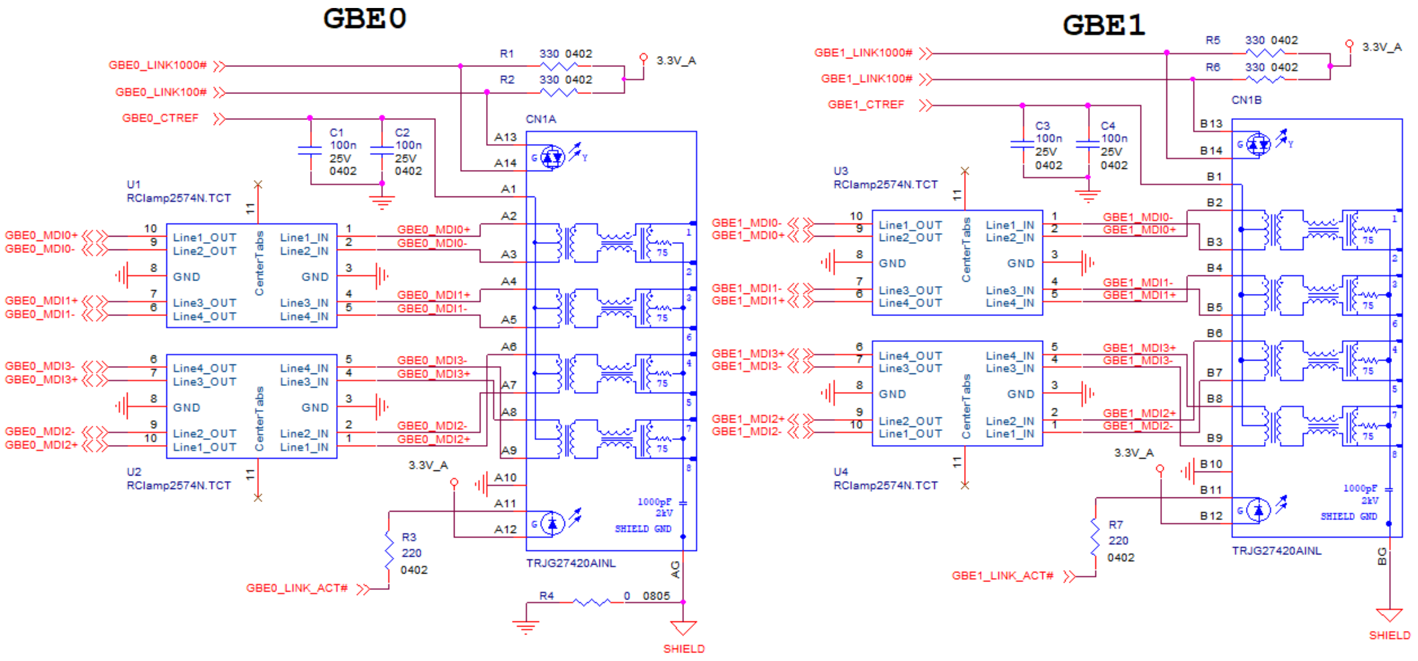
GBE1_LINK100#: Ethernet controller 100Mbps link indicator. Active Low Output signal, +3.3V_ALW electrical level

GBE1_LINK1000#: Ethernet controller 1Gbps link indicator. Active Low Output signal, +3.3V_ALW electrical level

GBE1_SDP: Software defined pin, directly managed by TI Gigabit Ethernet PHY transceiver #1. Bidirectional signal, +3.3V_ALW electrical level.

Please refer to the following schematics as an example of connection of Ethernet interface on the carrier board, with TVS diodes specifically designed to protect sensitive components which are connected to high-speed data and transmission lines from overvoltage caused by ESD. In this example, it is also present GBE_CTREF signal connected on pin #2 of the RJ-45 connector. TI Gigabit Ethernet PHY transceiver, however, doesn't need the analog powered centre tap, therefore the signal GBE_CTREF is not available on SMARC connector.

Please notice that if just a FastEthernet (i.e. 10/100 Mbps) is needed, then only MDI0 and MDI1 differential lanes are necessary, for both Gigabit Ethernet interfaces



3.2.1.15 CAN interface signals

Two CAN interfaces, directly managed by the Elkhart Lake processor, are available on SMARC card edge connector.

CAN0_TX: CAN Transmit Output for CAN Bus Channel 0. +1.8V_RUN electrical voltage level signal.

CAN0_RX: CAN Receive Input for CAN Bus Channel 0. +1.8V_RUN electrical voltage level signal.

CAN1_TX: CAN Transmit Output for CAN Bus Channel 1. +1.8V_RUN electrical voltage level signal.

CAN1_RX: CAN Receive Input for CAN Bus Channel 1. +1.8V_RUN electrical voltage level signal.

Please consider that it is not possible to connect the SMARC CAN interface to any CAN Bus directly, it is necessary to integrate a CAN Bus Transceiver in the Carrier board.

3.2.1.16 Watchdog

WDT_TIME_OUT#: Watchdog timer Output. +1.8V_DSW electrical level

3.2.1.17 GPIO signals

The Embedded controller MEC1705 GPIO interface provides general purpose input monitoring and output control, as well as many other features for the GPIO described on datasheet.

The signals involved in GPIO management are:

GPIO0: General Purpose I/O #0, +1.8V_DSW electrical level

GPIO1: General Purpose I/O #1, +1.8V_DSW electrical level

GPIO2: General Purpose I/O #2, +1.8V_DSW electrical level

GPIO3: General Purpose I/O #3, +1.8V_DSW electrical level

GPIO4: General Purpose I/O #4, +1.8V_DSW electrical level

GPIO5: General Purpose I/O #5, +1.8V_DSW electrical level

GPIO6: General Purpose I/O #6, +1.8V_DSW electrical level

GPIO7: General Purpose I/O #7, +1.8V_DSW electrical level

GPIO8: General Purpose I/O #8, +1.8V_DSW electrical level

GPIO9: General Purpose I/O #9, +1.8V_DSW electrical level

GPIO10: General Purpose I/O #10, +1.8V_DSW electrical level

GPIO11: General Purpose I/O #11, +1.8V_DSW electrical level

GPIO12: General Purpose I/O #12, +1.8V_DSW electrical level

GPIO13: General Purpose I/O #13, +1.8V_DSW electrical level

3.2.1.18 FuSa signals

As a factory alternative to GPIO signals, the module does provide functional safety functions through following signals:

OKNOK0: Output antivalent signal for error indication to the system. Intel® Safety Island has an error collection hub that receives errors from processor, classifies them into severity levels and reports them as an output state to the system through this signal. +1.8V_ALW electrical level. Combined with OKNOK1, the system will switch to safe state for any of following OKNOK0 / OKNOK1 states ("0" / "0" power off, "0" / "1" error state, "1" / "1" reset state), while is in normal operating state "OK" with "1" / "1" (no fault). "0" stands for low level (GND), while "1" stands for high level (+1.8V_ALW).

OKNOK1: Output antivalent signal for error indication to the system. Intel® Safety Island has an error collection hub that receives errors from processor, classifies them into severity levels and reports them as an output state to the system through this signal. +1.8V_ALW electrical level. Combined with OKNOK1, the system will switch to safe state for any of following OKNOK0 / OKNOK1 states ("0" / "0" power off, "0" / "1" error state, "1" / "1" reset state), while is in normal operating state "OK" with "1" / "1" (no fault). "0" stands for low level (GND), while "1" stands for high level (+1.8V_ALW).

ALERT#: Output signal indicating that a correctable error occurred. Active low signal, +3.3V_ALW electrical level with 4k7Ω pull up resistor

SPIS_CS#: SPI Slave chip select active low input, +1.8V_ALW electrical level

SPIS_SCLK: SPI Slave clock input, +1.8V_ALW electrical level

SPIS_MISO: SPI Slave Master In Slave Out, bi-directional data. +1.8V_ALW electrical level

SPIS_MOSI: SPI Slave Master Out Slave In, bi-directional data. +1.8V_ALW electrical level

CHXPMIC_EN: PMIC Enable override active high output signal, +1.8V_ALW electrical level

CHX_RLYSWITCH: Platform level relay switch override active high output signal, +1.8V_ALW electrical level

CHXOKNOX0: Output OK signal of other EHL channel, +1.8V_ALW electrical level

CHXOKNOK1: Output NOK signal of other EHL channel, +1.8V_ALW electrical level

SPIM_CS#: SPI Master chip select active low output, +1.8V_ALW electrical level

SPIM_SCLK: SPI Master clock output, +1.8V_ALW electrical level

SPIM_MISO: SPI Master Master In Slave Out, bi-directional data. +1.8V_ALW electrical level

In addition, the module does provide additional functional safety functions through following signals:

SPIM_MOSI: SPI Master Master Out Slave In, bi-directional data. +1.8V_ALW electrical level

THERMTRIP: Thermal Trip Output Signal, asserted by the processor to indicate a thermal trip event which may cause severe damage. Active high signal, +3.3V_ RUN electrical level with 10kΩ pull-up resistor

PROCHOT: Protection Output signal, asserted when the processor temperature monitoring sensor(s) detects that the processor has reached its maximum safe operating temperature. Active high signal, +3.3V_ RUN electrical level with 10kΩ pull-up resistor

FUSA_PWRFAIL#: FuSa Power Fail indication output signal. Active low signal, +3.3V_ RUN electrical level with 10kΩ pull-up resistor

CHXPMICEN: FuSa power input disabling signal, once asserted will disable 5V_DSW input signal. Active high signal, with 100kΩ pull-down resistor

3.2.1.19 Management pins

A set of signals are used by the module to communicate with carrier board for power management and indication status. Please refer to SMARC hardware specifications ver. 2.1 for more detailed informations.

The signals involved are:

VIN_PWR_BAD#: Power Bad indication signal from the Carrier Board, active low signal from a voltage detection circuit

CARRIER_PWR_ON: Power On. Command to the Carrier Board. Output is set to +1.8V_ALW electrical level with a 10k pull-down resistor

CARRIER_STBY#: Stand By command to the Carrier Board. Output, active low signal, is set to +1.8V_ALW electrical level with a 10k pull-down resistor

RESET_OUT#: General Purpose Reset. Output, active low signal, +1.8V_ALW electrical level with a 10k pull-down resistor

RESET_IN#: General Purpose Reset. Input, active low signal, +1.8_ALW electrical level with a 10k pull-up resistor

POWER_BTN#: Power Button. Input, active low signal, +1.8_DSW electrical level with a 10k pull-up resistor

SLEEP#: Sleep indicator from Carrier board. Input, active low signal, +1.8_ALW electrical level with a 10k pull-up resistor

LID#: LID Switch. Input, active low signal, +1.8_ALW electrical level with a 10k pull-up resistor

BATLOW#: Battery Low indication signal from the Carrier Board. Input, active low signal, +1.8V_DSW electrical level with a 10k pull-up resistor

CHARGING#: Battery Charging Input Signal from the Carrier Board. Input, active low signal, +1.8V_DSW electrical level with a 2k2 pull-up resistor

CHARGER_PRSNT#: Battery Charger Present input from the Carrier Board. Input, active low signal, +1.8V_DSW electrical level with a 2k2 pull-up resistor

TEST#: Signals used to invoke from Carrier Board specific test function(s). Input, active low signal, +1.8V_DSW electrical level with a 10k pull-up resistor. At the moment, this function is not implemented and reserved for its use in the future.

SMB_ALERT_1V8#: SM Bus Alert# (interrupt) signal. Input, active low signal, +1.8V_DSW electrical level with a 2k2 pull-up resistor

3.2.1.20 Boot Select

The following signals are active low and driven by open/ground circuitry on the carrier board.

BOOT_SEL0#: Boot Device Selection #0. Input, +1.8V_ALW electrical level with a 10k pull-up resistor

BOOT_SEL1#: Boot Device Selection #1. Input, +1.8V_ALW electrical level with a 10k pull-up resistor

BOOT_SEL2#: Boot Device Selection #2. Input, +1.8V_ALW electrical level with a 10k pull-up resistor

FORCE_RECOV#: Force recovery Mode. Input, +1.8_ALW electrical level with a 10k pull-up resistor

Chapter 4.
BIOS SETUP

- Aptio setup Utility
- Main setup menu
- Advanced menu
- Chipset menu
- Security menu
- Boot menu
- Save & Exit menu

4.1 Aptio setup Utility

Basic setup of the board can be done using American Megatrends, Inc. “Aptio Setup Utility”, that is stored inside an onboard SPI Serial Flash.

It is possible to access to Aptio Setup Utility by pressing the <ESC> key after System power up, during POST phase. On the splash screen that will appear, select “SCU” icon.

On each menu page, on left frame are shown all the options that can be configured.

Grayed-out options are only for information and cannot be configured.

Only options written in blue can be configured. Selected options are highlighted in white.

Right frame shows the key legend.

KEY LEGEND:

← / → Navigate between various setup screens (Main, Advanced, Security, Power, Boot...)

↑ / ↓ Select a setup item or a submenu

+ / - + and - keys allows to change the field value of highlighted menu item

<F1> The <F1> key allows displaying the General Help screen.

<F2> Previous Values

<F3> <F3> key allows loading Optimised Defaults for the board. After pressing <F3> BIOS Setup utility will request for a confirmation, before loading such default values. By pressing <ESC> key, this function will be aborted

<F4> <F4> key allows save any changes made and exit Setup. After pressing <F10> key, BIOS Setup utility will request for a confirmation, before saving and exiting. By pressing <ESC> key, this function will be aborted

<ESC> <Esc> key allows discarding any changes made and exit the Setup. After pressing <ESC> key, BIOS Setup utility will request for a confirmation, before discarding the changes. By pressing <Cancel> key, this function will be aborted

<ENTER> <Enter> key allows to display or change the setup option listed for a particular setup item. The <Enter> key can also allow displaying the setup sub-screens.

4.2 Main setup menu

When entering the Setup Utility, the first screen shown is the Main setup screen. It is always possible to return to the Main setup screen by selecting the Main tab.

In this screen, are shown details regarding BIOS version, Processor type, Bus Speed and memory configuration.

Three options, that are found at the end of list of details, can be configured, Language, Date and Time.

4.2.1 System Language / System Date / System Time

Entering System Language will list the available languages for the Setup Utility.

To change the system time and date Highlight System Time or System Date using the <Arrow> keys. Enter new values directly through the keyboard, or using + / - keys to increase / reduce displayed values. Press the <Enter> key to move between fields. The date must be entered in MM/DD/YY format. The time is entered in HH:MM:SS format.

Note: The time is in 24-hour format. For example, 5:30 A.M. appears as 05:30:00, and 5:30 P.M. as 17:30:00.

The system date is in the format mm/dd/yyyy.

4.3 Advanced menu

Menu Item	Options	Description
CPU Configuration	See submenu	CPU Configuration Parameters
Power & Performance	See submenu	Power & Performance Options
PCH-FW Configuration	See submenu	Configure Management Engine Technology Parameters
Intel® Time Coordinated Computing	See submenu	Intel® Time Coordinated Computing (Intel® TCC) options
Trusted Computing	See submenu	Trusted Computing Settings
ACPI Settings	See submenu	System ACPI parameters
S5 RTC Wake Settings		Enable system to wake from S5 using RTC alarm --> Enable/Disable System wake on alarm event
Serial Port Console Redirection	See submenu	Serial Port Console Redirection
AMI Graphic Output Protocol Policy	See submenu	User Selected Monitor Output by Graphic Output protocol
USB Configuration	See submenu	USB Configuration Parameters
Network Stack Configuration	See submenu	Network Stack Settings
NVMe Configuration	See submenu	NVMe Device Options Settings
SDIO Configuration	See submenu	SDIO Configuration Parameters
SMBIOS Information		SMBIOS Information
Main Thermal Configuration	See submenu	Main Thermal Configuration
LVDS Configuration	See submenu	LVDS Configuration
Embedded Controller	See submenu	Embedded Controller
RAM Disk Configuration	See submenu	Add/remove RAM disks
User Password Management		Handle user's password
Driver Health		Health Status for the Drivers/Controllers

4.3.1 CPU Configuration

Menu Item	Options	Description
CPU Configuration		Shows board's specific SoC information
CPU Flex Ratio Override	Disabled / Enabled	Enable/Disable CPU Flex Ratio Programming
CPU Flex Ratio Settings	[1…63]	This value must be between Max Efficiency Ratio (LFM) and Maximum non-turbo ratio set by Hardware (HFM)
Hardware Prefetcher	Disabled / Enabled	To turn on/off the MLC streamer prefetcher
Intel (VMX) Virtualization Technology	Disabled / Enabled	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology
PECI	Disabled / Enabled	Enable/Disable PECI
Active Processor Cores	All 1 2 3	Number of Cores to enable in each processor package
BIST	Disabled / Enabled	Enable/Disable BIST (Built-In Self Test) on reset
AP threads Idle Manner	HALT Loop MWAIT Loop RUN Loop	AP threads Idle Manner for waiting signal to run
AES	Disabled / Enabled	Enable/Disable AES (Advanced Encryption Standard)
MachineCheck	Disabled / Enabled	Enable/Disable MachineCheck
MonitorWait	Disabled / Enabled	Enable/Disable MonitorWait (MWAIT)
CPU SMM Enhancement	See Submenu	CPU SMM Enhancement
AC Split Lock	Disabled / Enabled	Enable/Disable AC Split Lock

4.3.2 Power & Performance

Menu Item	Options	Description
CPU - Power Management Control	See submenu	CPU – Power Management Control Options
GT - Power Management Control	See submenu	GT – Power Management Control Options

4.3.2.1 CPU - Power Management Control

Menu Item	Options	Description
Boot performance mode	Max Battery Max Non-Turbo Performance Turbo Performance	Select the performance state that the BIOS will set starting from reset vector
Intel® SpeedStep (tm)	Enabled / Disabled	Allows more than two frequencies ranges to be supported
Race to Halt (RTH)	Enabled / Disabled	Enable/Disable Race to Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-state faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)
Intel® Speed Shift Technology	Enabled / Disabled	Enable/Disable Intel® Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states
HwP Autonomous EPP Grouping	Enabled / Disabled	Enable EPP grouping (default bit 29 =0 , command 0x11). Autonomous will request the same values for all cores with same EPP. Disable EPP grouping (Bit 29 =1, command 0x11) autonomous will not necessarily request same values for all cores with same EPP
EPB override over PECI	Enabled / Disabled	Enable/Disable EPB override over PECI. Enable by sending pcode command 0x2b, subcommand 0x3 to 1. This will allow OOB EPB PECI override control
HwP fast MSR Support	Enabled / Disabled	Enable/Disable HwP Fast MSR Support for IA32_HWP_REQUEST MSR
HDC Control	Enabled / Disabled	This option allows HDC configuration. Disabled: Disable HDC Enabled: Can be enabled by OS if OS native support is available
View/Configure Turbo Options	See Submenu	View/Configure Turbo Options
CPU VR Settings	See Submenu	CPU VR Settings
Platform PL1 Enable	Enabled / Disabled	Enable/Disable Platform Power Limit 1 programming. If this option is enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window
Platform PL1 Power	[0…4095875]	Platform Power Limit 1 Power in Milli Watts. BIOS will round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For 12.50W, enter 12500. This setting will act as the new PL1 value for the Package RAPL algorithm.
Platform PL1Time Window	0 / 1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 10 / 12 / 14 / 16 / 20 / 24 / 28 / 32 / 40 /	Platform Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value. Indicates the time window over which Platform TDP value should be maintained

	48 / 56 / 64 / 80 / 96 / 112 / 128	
Platform PL2 Enable	Enabled / Disabled	Enable/Disable Platform Power Limit 2 programming. If this option is enabled, BIOS will program the default values for Platform Limit 2
Platform PL2 Power	[0…4095875]	Platform Power Limit 2 Power in Milli Watts. BIOS will round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For 12.50W, enter 12500. This setting will act as the new PL2 value for the Package RAPL algorithm.
Power Limit 4 Override	Enabled / Disabled	Enable/Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Poer Limit 4.
Power Limit 4	[0…4095875]	Platform Power Limit 4 in Milli Watts. BIOS will round to the nearest 1/8W when programming. For 12.50W, enter 12500. If the value is 0, BIOS leaves default value
Power Limit 4 Lock	Enabled / Disabled	Power Limit 4 MSR 601h Lock. When enabled PL4 configurations are locked during OS. When disabled PL4 configuration can be changed during OS
C states	Enabled / Disabled	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized
Enhanced C-states	Enabled / Disabled	Enable/Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-state
C-State Auto Demotion	Disabled / C1	Configure C-State Auto Demotion
C-State Un-demotion	Disabled / C1	Configure C-State Un-demotion
Package C-State Demotion	Enabled / Disabled	Package C-State Demotion
Package C-State Un-demotion	Enabled / Disabled	Package C-State Un-demotion
CState Pre-Wake	Enabled / Disabled	Disable – Sets bit 30 of POWER_CTL MSR (0x1FC) to 1 to disable the Cstate Pre-Wake
IO MWAIT Redirection	Enabled / Disabled	When set, will map IO_read instructions sent to IO registers. PMG_IO_BASE_ADDRBASE+offset to MWAIT (offset)
Package C State Limit	C0/C1 / C2 / C3 / C6 / C7 / C7S / C8 / C9 / C10 / Cpu Default / Auto	Maximum Package C State Limit Setting. Cpu Default: Leaves to factory default value Auto: Intializes to deepest available Package C State Limit
C6/C7 Short Latency Control (MSR 0x60B) C6/C7 Long Latency Control (MSR 0x60C) C8 Latency Control (MSR 0x633)	Time Unit (ns): 1 / 32 / 1024 / 32768 / 1048576 / 33554432 Latency: [0…1023]	Time Unit: Unit of measurement for IRTL value – bits [12:10] Latency: Interrupt Response Time Limit value – bits [9:0], Enter 0-1023

C9 Latency Control (MSR 0x634) C10 Latency Control (MSR 0x635)		
Thermal Monitor	Enabled / Disabled	Enable/Disable Thermal Monitor
Interrupt Redirection Mode Selection	Fixed Priority Round robin Hash Vector No Change	Interrupt Redirection Mode Select for logical Interrupts
Timed MWAIT	Enabled / Disabled	Enable/Disable Timed MWAIT Support
Custom P-state Table		Add Custom P-state Table --> Sets the number of custom P-states. At least 2 states must be present
EC Turbo Control Mode	Enabled / Disabled	Enable/Disable EC Turbo Control mode
AC Brick Capacity	90W AC Brick 65W AC Brick 75W AC Brick	Specify the AC Brick capacity
EC Polling Period	[1…255]	Count 1 to 255 for a range of 10ms to 2.55 seconds (1 count = 10ms)
EC Guard Band Value	[1…20]	Count 1 to 20 for a range of 1 Watt to 20 Watts
EC Algorithm Selection	[1…10]	Count 1 to 10 for Algorithm Selection
Energy Performance Gain	Enabled / Disabled	Enable/Disable Energy Performance Gain
EPG DIMM Idd3N	26 (default)	Active standby current (Idd3N) in milliamps from datasheet. Must be calculated on a per DIMM basis
EPG DIMM Idd3P	11 (default)	Active power-down current (Idd3P) in milliamps from datasheet. Must be calculated on a per DIMM basis
CPU Lock Configuration	See submenu	CPU Lock Configuration

4.3.2.1.1 View/Configure Turbo Options

Menu Item	Options	Description
Current Turbo Settings		Shows cores' specific Turbo information
Energy Efficient P-state	Enabled / Disabled	Enable/Disable Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 ECX[3] will read 0 indicating no support for Energy Efficient policy setting. When set to 1 will enable access to ENERGY_PERFORMANCE_BIAS MSR
Package Power Limit MSR Lock	Enabled / Disabled	Enable/Disable locking of Package Power Limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register

Power Limit 1 Override	Enabled / Disabled	Enable/Disable Power Limit 1 override. If this option is disabled, BIOS will program the default values for Power Limit 1 and Power Limit 1 Time Window.
Power Limit 1	[0…4095875]	Platform Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP Limit. If value is 0, BIOS leaves default value
Power Limit 1 Time Window	Enabled / Disabled	Platform Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value. Indicates the time window over which Platform TDP value should be maintained
Power Limit 2 Override	Enabled / Disabled	Enable/Disable Power Limit 1 override. If this option is disabled, BIOS will program the default values for Power Limit 2
Power Limit 2	[0…4095875]	Platform Power Limit 2 in Milli Watts. BIOS will round to the nearest 1/8W when programming. If the value is 0, BIOS will program this value as 1.25*TDP. For 12.50W, enter 12500. Processor applies policies such that the package power does not exceed this limit
1-Core Ratio Limit Override	[0…83]	1-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 1-Core Ratio Limit must be grater than or equal to 2-Core Ratio Limit, 3-Core Ratio Limit, 4-Core Ratio Limit
2-Core Ratio Limit Override	[0…83]	2-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 2-Core Ratio Limit must be less than or equal to 1-Core Ratio Limit
3-Core Ratio Limit Override	[0…83]	3-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 3-Core Ratio Limit must be less than or equal to 1-Core Ratio Limit
4-Core Ratio Limit Override	[0…83]	4-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 4-Core Ratio Limit must be less than or equal to 1-Core Ratio Limit
Energy Efficient Turbo	Enabled / Disabled	Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overclocking situations where turbo frequency must remain constant. Otherwise, leave enabled.

4.3.2.1.2 CPU VR Settings

Menu Item	Options	Description
PSYS Slope	[0…200]	PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9
PSYS Offset	[0…63999]	PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. Uses BIOS VR mailbox command 0x9
PSYS Prefix	+ / -	Sets the offset value as positive or negative

PSYS Pmax Power	[0…8192]	PSYS Pmax power, defined in 1/8 Watt increments. Range 0-8192. For a Pmax of 125W, enter 1000. 0 = AUTO. Uses BIOS VR mailbox command 0xB
Acoustic Noise Settings	See submenu	Configure Acoustic Noise Settings for IA, GT and SA domains
VccIn VR Settings	See submenu	VccIn VR Settings
RFI Settings	See submenu	RFI Settings

4.3.2.1.2.1 Acoustic Noise Settings

Menu Item	Options	Description
Acoustic Noise Mitigation	Enabled / Disabled	Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state
Disable Fast PKG C State Ramp for VccIn Domain	FALSE / TRUE	This option needs to be configured to reduce acoustic noise during deeper C state. FALSE: Don't disable Fast ramp during deeper C state; TRUE: Disable Fast ramp during deeper C state
Slow Slew Rate for VccIn Domain	Fast/2 Fast/4 Fast/8 Fast/16	Set VR VccIn Slow Slew Rate for Deep Package C state ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise

4.3.2.1.2.2 VccIn VR Settings

Menu Item	Options	Description
VR Config Enable	Enabled / Disabled	VR Config Enable
AC Loadline	[0…6249]	AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2
DC Loadline	[0…6249]	DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2
PS Current Threshold1	[0…512]	PS Current Threashold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS Current Threshold2	[0…512]	PS Current Threashold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS Current Threshold3	[0…512]	PS Current Threashold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3

PS3 Enable	Enabled / Disabled	PS3 Enable/Disable. 0 – Disabled, 1 – Enabled. Uses BIOS VR mailbox command 0x3
PS4 Enable	Enabled / Disabled	PS4 Enable/Disable. 0 – Disabled, 1 – Enabled. Uses BIOS VR mailbox command 0x3
IMON Slope	[0…200]	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4
IMON Offset	[0…63999]	IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. Uses BIOS VR mailbox command 0x4
IMON Prefix	+ / -	Sets the offset value as positive or negative
VR Current Limit	[0…512]	Voltage Regulator Current Limit (Icc Max). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. A value of 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6
TDC Enable	Enabled / Disabled	TDC Enable. 0 – Disable, 1 – Enable
TDC Current Limit	[0…32767]	TDC Current Limit, defined in 1/8 increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A
TDC Time Window	[1…8, 10]	TDC Time Window, value in milliseconds. 1ms is default. Range from 1ms to 1ms, except for 9ms. 9ms has no valid encoding in the MSR definition
TDC Lock	Enabled / Disabled	TDC Lock

4.3.2.1.2.3 RFI Settings

Menu Item	Options	Description
RFI Current Frequency		Shows current RFI Frequency setting
RFI Frequency	[1300…1600]	Set desired RFI Frequency, in increments of 100KHz. The RFI Frequency Range is between 130 MHz to 160 MHz, and the default h/w frequency is 139.6 MHz. For a frequency of 139.6 MHz, enter 1396
RFI Spread Spectrum	[0…100]	Adjust the Spread Spectrum, in increments of 0.1%. For a spread of 5.0%, enter 50. The value of 0 will disable the FIVR FRI Spread Spectrum, Range 0-100 (0.0% to 10.0%)

4.3.2.1.3 CPU Lock Configuration

Menu Item	Options	Description
CFG Lock	Enabled / Disabled	Configure MSR 0xE2[15], CFG Lock bit
Overclocking Lock	Enabled / Disabled	Enable/Disable Overclocking Lock (BIT 20) in FLEX_RATIO(194) MSR

4.3.2.2 GT- Power Management Control

Menu Item	Options	Description
Maximum GTT frequency	Default Max Frequency / 100MHz / … *List of 50MHz increments* … / 1200MHz	Maximum GT frequency limited by the user. Choose between 200MHz (RPN) and 400MHz (RP0). Value beyond the range will be clipped to min/max supported by SKU
Disable Turbo GT frequency	Enabled / Disabled	Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited

4.3.3 PCH-FW Configuration

Menu Item	Options	Description
ME Firmware information		Shows ME Firmware specific information
ME State	Enabled / Disabled	When Disabled ME will be put into ME Temporarily Disabled Mode
ME Unconfig on RTC Clear	Enabled / Disabled	When Disabled ME will not be unconfigured on RTC Clear
Comms Hub Support	Enabled / Disabled	Enable/Disable support for Comms Hub
JHI Support	Enabled / Disabled	Enable/Disable Intel® DAL Host Interface Service (JHI)
Core Bios Done Message	Enabled / Disabled	Enable/Disable Core Bios Done message sent to ME
Firmware Update Configuration	See submenu	Configure Management Engine Technology Parameters
PTT Configuration	See submenu	Configure PTT
FIPS Configuration	See submenu	FIPS Mode help
ME Debug Configuration	See submenu	Configure ME debug options. NOTE: This menu is provided testing purposes. It is recommended to leave the options in their default states
Anti-Rollback SVN Configuration	See submenu	Configure Anti-Rollback SVN
OEM Key Revocation Configuration	See submenu	Configure OEM Key Revocation

4.3.3.1 Firmware Update Configuration

Menu Item	Options	Description

ME FW Image Re-Flash	Enabled / Disabled	Enable/Disable ME FW Image Re-Flash function
FW Update	Enabled / Disabled	Enable/Disable ME FW Update function

4.3.3.2 PTT Configuration

Menu Item	Options	Description
TPM Device Selection	dTPM / PTT	Selects TPM device: PTT or dTPM. PTT – Enables PTT in SkuMgr dTPM 1.2 – Disables PTT in SkuMgr Warning ! PTT/dTPM will be disabled and all data saved on it will be lost

4.3.3.3 FIPS Configuration

Menu Item	Options	Description
FIPS Mode Select	Enabled / Disabled	FIPS Mode configuration
FIPS Mode information		Shows FIPS Mode specific information

4.3.3.4 ME Debug Configuration

Menu Item	Options	Description
HECI Timeous	Enabled / Disabled	Enable/Disable HECI Send/Receive Timeouts
Force ME DID Init Status	Enabled / Disabled	Forces the DID Initialization Status value
CPU Replaces Polling Disable	Enabled / Disabled	Setting this option disables CPU replacement polling loop
ME DID Message	Enabled / Disabled	Enable/Disable ME DID Message (disable will prevent the DID message from being sent)
HECI Message check Disable	Enabled / Disabled	Settings this option disables message check for Bios Boot Path when sending
MBP HOB Skip	Enabled / Disabled	Setting this option will skip MBP HOB
HECI2 Interface Communication	Enabled / Disabled	Adds and Removes HECI2 Device from PCI space
KT Device	Enabled / Disabled	Enable/Disable KT Device
DOI3 Setting for HECI Disable	Enabled / Disabled	Setting this option disables setting DOI3 bit for all HECI devices
MCTP Broadcast Cycle	Enabled / Disabled	Enable/Disable Management Component Transport Protocol Broadcast Cycle and Set PMT as Bus Owner

4.3.3.5 Anti-Rollback SVN Configuration

Menu Item	Options	Description
Automatic HW-Enforced Anti-Rollback SVN	Enabled / Disabled	When enabled, hardware-enforced Anti-Rollback mechanism is automatically activated: once ME FW was successfully run on a platform, FW with lower ARB-SVN will be blocked from execution
Set HW-Enforced Anti-Rollback for Current SVN	Enabled / Disabled	Enable hardware-enforced Anti-Rollback mechanism for current ARB-SVN value. FW with lower ARB-SVN will be blocked from execution. The value will be restored to disable after the command is sent

4.3.3.6 OEM Key Revocation Configuration

Menu Item	Options	Description
Automatic OEM Key Revocation	Enabled / Disabled	When enabled, BIOS will automatically send HECI command to revoke OEM keys
Invoke OEM Key Revocation	Enabled / Disabled	A HECI command will be sent to revoke OEM keys

4.3.4 Intel® Time Coordinated Computing

Menu Item	Options	Description
Intel® TCC Mode	Enabled / Disabled	Enables or Disables Intel® TCC mode. When enabled, this will modify system settings to improve real-time performance. The full list of settings and their current state are displayed below when Intel® TCC mode is enabled.
Software SRAM	Enabled / Disabled	Enables or Disables Software SRAM. Enable will allocate 1 way of LLC; if Cache Configuration subreagion is available, it will allocate based on the subregion.
Data Streams Optimizer	Enabled / Disabled	Enables or Disables Data Streams Optimizers (DSO). Enable will utilize DSO Subregion to tune system. DSO settings supercede Intel® TCC Mode settings that overlap between the two.
TCC Error Log	Enabled / Disabled	Enables or Disables TCC Error Log. Enable will record errors from TCC flow in memory.
Intel® TCC Authentication Menu	See submenu	Intel® TCC Authentication Menu options
IO Fabric Low Latency	Enabled / Disabled	Enables or Disables IO Fabric Low Latency. This will turn off some power management in the PCH IO fabrics. This option provides the most aggressive IO Fabric performance settings S3 state is not supported.
GT CLOS	Enabled / Disabled	Enables or Disables Graphics Technology (GT) Class of Service. Enable will reduce Gfx LLC allocation to minimize impact of Gfx workload on LLC.
RAPL PL 1 enable		Memory RAPL PL 1 settings

RAPL PL 2 enable		Memory RAPL PL2 settings

4.3.5 Trusted computing

Menu Item	Options	Description
Security Device Support	Enabled / Disabled	Enables or Disables BIOS support for security device. OS will not show the Security Device. TCG EFI protocol and INT1A interface will not be available. When enabled all the following items will be available.
SHA256 PCR Bank	Enabled / Disabled	Enables or Disables SHA256 PCR Bank
SHA384 PCR Bank	Enabled / Disabled	Enables or Disables SHA384 PCR Bank
SM3_256 PCR Bank	Enabled / Disabled	Enables or Disables SM3_256 PCR Bank
Pending Operation	None / TPM Clear	Schedule an Operation for the Security Device. NTE: your Computer will reboot during restart in order to change State of Security Device.
Platform Hierarchy	Enabled / Disabled	Enables or Disabled the Platform Hierarchy
Storage Hierarchy	Enabled / Disabled	Enables or Disabled the Storage Hierarchy
Endorsement Hierarchy	Enabled / Disabled	Enables or Disabled the Endorsement Hierarchy
Physical Presence Spec Version	1.2 / 1.3	Select to tell OS to support PPI Spec Version 1.2 or 1.3. Please note that some HCK tests might not support 1.3
Device Select	Auto TPM 1.2 TPM 2.0	TPM 1.2 will restrict the support to TPM 1.2 devices only, TPM 2.0 will restrict the support to TPM 2.0 devices only, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated

4.3.6 ACPI Settings

Menu Item	Options	Description
Enable ACPI Auto Configuration	Disabled / Enabled	Enables or Disables BIOS ACPI Auto Configuration. The following menu items will appear only when this menu item is Disabled
Enable Hibernation	Disabled / Enabled	Enables or disables system ability to Hybernate (OS/S4 Sleep State). This option may be not effective with some OS.
ACPI Sleep State	Suspend Disabled S3 (Suspend to RAM)	Select the highest ACPI Sleep state the system will enter when the SUSPEND button is pressed.
Lock Legacy resources	Disabled / Enabled	Enables or Disables Lock of Legacy resources

4.3.7 Serial Port Console Redirection

Menu Item	Options	Description
COMx		
Console redirections	Enabled / Disabled	Enables or Disables the Console redirection. When enabled the following item will appear
Console Redirection Settings	See Submenu	The settings specifies how the host and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings
Console redirections EMS	Enabled / Disabled	Enables or Disables the Console redirection. When enabled the following item will appear
Console Redirection Settings	See Submenu	The settings specifies how the host and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings

4.3.7.1 *Console Redirection Settings (COMx)*

Menu Item	Options	Description
Terminal Type	VT100 VT100+ VT-UTF8 ANSI	Emulation: ANSI: Extended ASCII Char set. VT100: ASCII Char set. VT100+: extends VT100 to support colour, function keys, etc. VT-UTF8: uses UTF8 encoding to map Unicode chars onto 1 or more bytes
Bits per second	9600 / 19200 / 38400 / 57600 / 115200	Select Serial port Transmission Speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data bits	7 / 8	Set Console Redirection data bits
Parity	None Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the number of 1s in the data bits is even. Odd: parity bit is 0 if the number of 1s in the data bits is odd. Mark: parity bit is always 1. Space: parity bit is always 0. Mark and Space do not allow for error detection
Stop bits	1 / 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit
Flow Control	None Hardware RTS/CTS	Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses RTS# / CTS# lines to send the start / stop signals.
VT-UTF8 Combo Key Support	Enabled / Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals

Recorder Mode	Enabled / Disabled	When this mode is enabled, only text will be sent. This is to capture Terminal data.
Resolution 100x31	Enabled / Disabled	Enables or disables extended terminal resolution
Putty Keypad	VT100 / Intel Linux / XTERMR6 / SCO / ESCN /VT400	Select FunctionKey and KeyPad on Putty

4.3.7.2 *Console Redirection Settings (EMS)*

Menu Item	Options	Description
Out-of-Band Mgmt Port	COM0 COM1	Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port
Terminal Type EMS	VT100 VT100+ VT-UTF8 ANSI	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console redirection Settings page, for more help with Terminal Type/Emulation
Bits per second	9600 / 19200 / 57600 / 115200	Select Serial port Transmission Speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Flow Control	None Hardware RTS/CTS Software Xon/Xoff	Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

4.3.8 AMI Graphic Output Protocol Policy

Menu Item	Options	Description
Output Select	*List of available / connected module's video interfaces*	Output Interface, this menu is visible when more than one interface is available
Brightness Settings	20/40/60/80/100/120/140/160/180/200/220/240/255	Set GOP Brightness value
BIST Enable	Enabled / Disabled	Starts or stops the BIST on the integrated display panel

4.3.9 USB Configuration

Menu Item	Options	Description

Legacy USB Support	Enabled / Disabled / Auto	Enables Legacy USB Support. AUTO Option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI hand-off	Enabled/ Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enabled/ Disabled	Enables or disables USB Mass Storage Driver Support
USB Transfer time-out	1 sec / 5 sec / 10 sec / 20 sec	Sets the time-out value for Control, Bulk and Interrupt transfers
Device reset time-out	10 sec / 20 sec / 30 sec / 40 sec	USB mass storage device Start Unit command time-out
Device power-up delay	Auto / Manual	Sets the maximum time that the device will take before it properly reports itself to the Host controller. 'Auto' uses the default vale (for a Root port it is 100ms, for a Hub port the delay is taken from the Hub descriptor).
Device power-up delay in seconds	[1..40]	Delay range in seconds, in one second increment, visible when delay is set to Manual

4.3.10 Network Stack configuration

Menu Item	Options	Description
Network Stack	Enabled / Disabled	Enables or disables UEFI Network Stack. When enabled, following menu items will appear
Ipv4 PXE Support	Enabled / Disabled	Enables or disables IPV4 PXE Boot Support. If disabled, IPV4 PXE boot option will not be created
Ipv4 HTTP Support	Enabled / Disabled	Enables or disables IPV4 HTTP Boot Support. If disabled, IPV4 HTTP boot option will not be created
Ipv6 PXE Support	Enabled / Disabled	Enables or disables IPV6 PXE Boot Support. If disabled, Ipv6 PXE boot option will not be created
Ipv6 HTTP Support	Enabled / Disabled	Enables or disables IPV6 HTTP Boot Support. If disabled, Ipv6 HTTP boot option will not be created
PXE boot wait time	[0..5]	Wait time to press ESC key to abort the PXE boot
Media detect count	[1..50]	Number of times that the presence of media will be checked

4.3.11 NVMe configuration

Menu Item	Options	Description
List of NVMe devices found		

4.3.12 SDIO configuration

Menu Item	Options	Description

SDIO Access Mode	Auto ADMA SDMA PIO	Auto Option: Access the SD Device in DMA mode if the controller supports it, otherwise in PIO Mode. DMA Option: Access the SD Device in DMA mode ADMA Option: Access the SD Device in Advanced DMA mode PIO Option: Access the SD Device in PIO mode
List of SDIO devices found	Auto Floppy Forced FDD Hard Disk	Mass storage device emulation type. 'Auto' enumerates devices less than 530Mb as floppies. Forced FDD option can be used to force HDD formatted drive to boot as FDD.

4.3.13 Main Thermal Configuration

Menu Item	Options	Description
Critical Temperature (°C)	90 / 95 / 100 / 105 / 110 / 115 / 117 / 119 / Disabled	Above this threshold, an ACPI aware OS performs a critical shut down. Allowed range is from 90°C to 119°C included or disabled.
Passive Cooling Temperature (°C)	80 / 85 / 90 / 95 / 100 / 105 / 107 / 109 / Disabled	Above this threshold, an ACPI aware OS begins to lower the CPU speed. Allowed range is from 80 to 109 °C included or disabled.
TC1	1 (default)	Thermal Constant 1: part of the ACPI Passive Cooling Formula
TC2	1 (default)	Thermal Constant 2: part of the ACPI Passive Cooling Formula
TSP (tenths of second)	5 (default)	Period of temperature sampling when Passive Cooling

4.3.14 LVDS Configuration

Menu Item	Options	Description
LVDS interface	Enabled / Disabled	Enables or Disables the LVDS interface. When enabled all the following parameters will appear
Edid Mode	External / Default / Custom	Select the source (EDID, Extended Display Identification Data) to be used for the internal flat panel. Depending on the setting chosen, only some of the following option or none will appear.
EDID	640x480 / 800x480 / 800x600 / 1024x600 / 1024x768 / 1280x720 / 1280x800 / 1280x1024 / 1366x768 / 1400x900 / 1600x900 / 1680x1050 / 1920x1080	Only available when Edid Mode is set to "default". Select a software resolution (EDID settings) to be used for the internal flat panel.
Color Mode	VESA 24bpp / JEIDA 24bpp / 18 bpp	Select the color depth of LVDS interface. For 24-bit color depth, it is possible to choose also the color mapping on LVDS channels, i.e. if it must be VESA-compatible or JEIDA compatible.

Interface	Single Channel / Dual Channel	Allows configuration of LVDS interface in Single or Dual channel mode
DE Polarity	Active High / Active Low	Data Enable Polarity
V-Sync Polarity	Negative / Positive	Vertical Sync Polarity
H-Sync Polarity	Negative / Positive	Horizontal Sync Polarity
LVDS Advanced Options	See Submenu	LVDS Advanced Options Configurations

4.3.14.1 LVDS Advanced options

Menu Item	Options	Description
Spreading Depth	No Spreading / 0.5% / 1.0% / 1.5% / 2.0% / 2.5%	Sets percentage of bandwidth of LVDS clock frequency for spreading spectrum
Output Swing	150 mV / 200 mV / 250 mV / 300 mV / 350 mV / 400 mV / 450 mV	Sets the LVDS differential output swing
T3 Timing	[0..255]	Minimum T3 timing of panel power sequence to enforce (expressed in units of 50ms). Default is 10 (500ms)
T4 Timing	[0..255]	Minimum T4 timing of panel power sequence to enforce (expressed in units of 50ms). Default is 2 (100ms)
T12 Timing	[0..255]	Minimum T12 timing of panel power sequence to enforce (expressed in units of 50ms). Default is 20 (1s)
T2 Delay	Enabled / Disabled	When Enabled, T2 is delayed by 20ms ± 50%
T5 Delay	Enabled / Disabled	When Enabled, T5 is delayed by 20ms ± 50%
P/N Pairs Swapping	Enabled / Disabled	Enable or disable LVDS Differential pairs swapping (Positive ⇔ Negative)
Pairs Order Swapping	Enabled / Disabled	Enable or disable channel differential pairs order swapping (A ⇔ D, B ⇔ CLK, C ⇔ C)
Bus Swapping	Enabled / Disabled	Enable or disable Bus swapping (Odd ⇔ Even)
Firmware PLL	0: +/- 1.56% 1: +/- 3.12% 2: +/- 6.25% 3: +/- 12.5% 4: +/- 25% 5: +/- 50% 6: +/- 100%	Firmware PLL range

4.3.15 Embedded Controller

Menu Item	Options	Description
Embedded Controller information		Shows Embedded Controller specific information
Power Fail Resume Type	Always ON Always OFF Last State	Specify what state to go to when power is re-applied after a power failure (G3 state). If Batteryless Operation, the chipset always powers on after a power failure: Always OFF Resume Type or Last State when Last State was OFF will therefore require an immediate shutdown.
No C-MOS battery handling	Enabled / Disabled	In systems with no C-MOS battery, the chipset always powers on after a power failure: Always OFF Resume Type or Last State when Last State was OFF will therefore require an immediate shutdown.
LID_BTN# Configuration	Force Open Force Closed Normal Polarity Inverted Polarity	Configures the LID_BTN# signal as always open or closed, no matter the pin level, or configures the pin polarity: High = Open (Normal), Low = Open (Inverted)
LID_BTN# Wake Configuration	No Wake Only From S3 Wake From S3/S4/S5	Configures LID_BTN# wake capability (when not forced to Open or Closed). According to the pin configuration, when the LID is open it can cause a system wake from a sleep state.
OUT 80 serial redirection port	None / 1 / 2 / 1+2	Select on which E.C. UART(s) to redirect OUT 80 (Post Codes)
Hardware Monitor		Shows Monitored Hardware parameters and settings
Reset Causes Handling	See Submenu	Reset Causes Handling
Super IO Configuration	See Submenu	Super IO Configuration
External FAN/PWM Settings	See Submenu	Visible when PWM/FAN Management is Enabled under SMARC Related Configuration
Watchdog Configuration		Configure the Watchdog Timer --> Disables/Enables the Watchdog Timer Mechanism
GPIO Configurations	See Submenu	GPIO Configurations
MAC address(es) visualization		MAC address(es) visualization
SMARC Related Configuration	See Submenu	Configuration options related to SMARC standard
USB Port Enabling		USB Port enabling --> Disables/Enables VBUS on carrier board for each USB Port

4.3.15.1 Reset Causes Handling

Menu Item	Options	Description
Reset Button Pressed		Happened / Not Happened

Clear from log	Enabled / Disabled	If Enabled will require system reset
WDT Timeout Expired		Happened / Not Happened
Power Failure		Happened / Not Happened
Clear from log	Enabled / Disabled	If Enabled will require system reset
E.C. soft reset		Happened / Not Happened
Clear from log	Enabled / Disabled	If Enabled will require system reset

4.3.15.2 Super IO Configuration

Menu Item	Options	Description
Serial Port x	Enabled / Disabled	
Address	0x3F8 / 0x3E8 / 0x2F8 / 0x2F0 / 0x2E8 / 0x2E0 / 0x2A8 / 0x2A0 / 0x288 / 0x280	Serial Port IO Base Address
IRQ	3 / 4 / 5 / 6 / 7 / 10 / 11 / 14 / 15	Serial Port IRQ

4.3.15.3 External FAN/PWM Settings

Menu Item	Options	Description
FAN_PWMOUT device type	3-WIRE FAN 4-WIRE FAN Generic PWM	Specifies if FAN_PWMOUT is connected to a 3-wire or 4-wire FAN or to a generic PWM
Automatic Temperature FAN Control	Enabled / Disabled	Disable/Enable Thermal Feed-back FAN Control
FAN PWM Frequency	[1..60000]	Sets the frequency of the FAN_PWMOUT signal. Typical values are 100 for a 3-wire device and 20000 for a 4-wire one
FAN Duty Cycle (%)	[0..100]	Sets the Duty Cycle of the FAN_PWMOUT signal

4.3.15.4 GPIO Configuration

Menu Item	Options	Description
GPIOx		

Configuration	Input Output Low Output High Output Last	Configure pin as input or output with a fixed starting value. Last means no changes with respect to the last boot

4.3.15.5 SMARC Related Configuration

Menu Item	Options	Description
HD Audio Reset	Enabled / Disabled	Enabling this option GPIO4 will be used for HD Audio Reset. GPIO4 --> HDA_RST#
PWM/FAN Management	Enabled / Disabled	Enabling this option GPIO5 will be used for PWM/FAN Output. GPIO5 --> PWM_OUT
Tachometer	Enabled / Disabled	Enabling this option GPIO6 will be used for Tachometer Input. GPIO6 --> TACHIN

4.3.16 RAM Disk Configuration

Menu Item	Options	Description
Disk Memory Type:	Boot Service Data Reserved	Specifies type of memory to use from available memory pool in system to create a disk
Create Raw		Create a raw RAM disk
Create from file		Create a RAM disk from a given file
Remove selected RAM disk(s)		Remove selected RAM disks

4.4 Chipset menu

Menu Item	Options	Description
System Agent (SA) Configuration	See Submenu	System Agent (SA) Parameters
PCH-IO Configuration	See Submenu	PCH Parameters

4.4.1 System Agent (SA) Configuration

Menu Item	Options	Description
Memory Configuration		Memory Configuration Parameters
Graphics Configuration	See Submenu	Graphics Configuration

4.4.1.1 Graphics Configuration

Menu Item	Options	Description
Graphics Turbo IMON Current	[14..31]	Graphics Turbo IMON Current values supported (14 – 31)
Skip Scanning of External Gfx Card	Enabled / Disabled	If Enabled, it will not scan for External Gfx Card on PEG and PCH PCIE ports
Primary Display	Auto / IGFX / PEG / PCI	Set which graphics device should be the Primary Display
External Gfx Card Primary Display Conf.	Auto / PCIEx	External Gfx Card Primary Display Configuration --> Select Auto or Primary PCIe
Internal Graphics	Auto / Disabled / Enabled	Keep IGFX enabled based on the setup options
GTT Size	2 MB / 4 MB / 8 MB	Select the GTT (Graphics Translation Table) Size
Aperture Size	256 MB	Use this item to set the total size of Memory that must be left to the GFX Engine
PSMI SUPPORT	Enabled / Disabled	PSMI Enabled / Disabled
DVMT Pre-Allocated	64M / 96M / 128M / 160M / 192M / 224M / 256M / 288M / 320M / 352M / 384M / 416M / 448M / 480M / 512M	Select DVMT5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphic Device
DVMT Total Gfx Mem	128M / 256M / MAX	Select the size of DVMT (Dynamic Video Memory) 5.0 that the Internal Graphics Device will use

DiSM Size (GB)	[0..7]	DiSM Size for 2LM Sku
Intel Graphics Pei Display Peim	Enabled / Disabled	Enable / Disable Pei (Early) Display
VDD Enable	Enabled / Disabled	Enable / Disable forcing of VDD in the BIOS
Configure GT for use	Enabled / Disabled	Enable / Disable GT configuration in BIOS
PAVP Enable	Enabled / Disabled	Enable / Disable Protected Audio Video Playback (PAVP)
Cdynmax Clamping Enable	Enabled / Disabled	Enable / Disable Cdynmax Clamping
Cd Clock Frequency	172.8 MHz / 307.2 MHz / 556.8 MHz / 652.8 MHz / Max CdClock freq based on Reference Clk	Select the highest CD Clock frequency supported by the platform
GT PM Support	Enabled / Disabled	Enable / Disable GT Power Management Support
Skip Full CD Clock Init	Enabled / Disabled	Enabled: Skip Full CD clock initialization; Disabled: Initialize the full CD clock if not initialized by Gfx PEIM
VBT Select	eDP / MIPI	Select VBT for GOP Driver
IUER Button Enable	Enabled / Disabled	Enable / Disable IUER Button Functionality
LCD Control	See Submenu	

4.4.1.2 LCD Control

Menu Item	Options	Description
Primary IGFX Boot Display	VBIOS Default EFP LFP EFP3 EFP2 EFP4	Select the Video Device which will be activated during POST. This has no effect if external graphics present. Secondary boot display selection will appear based on your selection. VGA modes will be supported only on primary display
LCD Panel Type	VBIOS Default 640x480 LVDS 800x600 LVDS 1024x768 LVDS 1280x1024 LVDS 1400x1050 LVDS 1 1400x1050 LVDS 2 1600x1200 LVDS	Select LCD panel used by Internal Graphics Device by selecting the appropriate setup item

	1280x768 LVDS 1680x1050 LVDS 1920x1200 LVDS 1600x900 LVDS 1280x800 LVDS 1280x600 LVDS 2048x1536 LVDS 1366x768 LVDS	
Panel Scaling	Auto Off Force Scaling	Select the LCD panel scaling option used by the Internal Graphics Device
Backlight Control	PWM Inverted PWM Normal	Backlight Control Settings
Active LFP	*List of active options*	Select the Active LFP Configuration. No LVDS: VBIOS does not enable LVDS Int-LVDS: VBIOS enables LVDS driver by Integrated encoder SDV0 LVDS: VBIOS eables LVDS driver by SDV0 encoder No eDP: VBIOS does not enable eDP eDP Port-A: LFP Driven by Int-DisplayPort encoder from Port-A
Panel Colour Depth	18 bit / 24 bit	Select the LFP Panel Color Depth
Backlight Brightness	[0..255]	Set Panel Brightness

4.4.2 PCH-IO Configuration

Menu Item	Options	Description
PCI Express Configuration	See submenu	PCI Express Configuration Settings
SATA Configuration	See submenu	SATA Device Options Settings
USB Configuration	See submenu	USB Configuration Settings
Security Configuration	See submenu	Security Configuration Settings
HD Audio Configuration	See submenu	HD Audio Subsystem Configuration Settings
Seriallo Configuration	See submenu	Seriallo Configuration Settomgs
SCS Configuration	See submenu	Storage and Communication Subsystem (SCS) Configuration

PSE Configuration	See submenu	Programmable Service Engine (PSE) Configuration
TSN GBE Configuration	See submenu	Time Sensitive Network GBE Configuration
PCle Ref Pll SSC	Auto / 0.0% / 0.1% / 0.2% / 0.3% / 0.4% / 0.5% / Disabled	Pcie Ref Pll SSC Percentage. AUTO – Keep hw default, no BIOS override.
Flash Potection Range Registers (FPRR)	Enabled / Disabled	Enable Flash Protection Range Registers
PinCntrl Driver GPIO Scheme	Enabled / Disabled	Enable/Disable PinCntrl Driver GPIO Scheme

4.4.2.1 PCI Express Configuration

Menu Item	Options	Description
DMI Link ASPM Control	Disabled / L0s / L1 / LosL1 / Auto	The control of Active State Power Management of the DMI Link
Compliance Mode	Enabled / Disabled	Enable when using Compliance Load Board
PCI Exopress Root Port x	See submenu	Sets the parameters for each single PCI-e Root Port

4.4.2.1.1 *PCI Express Root Port x*

Menu Item	Options	Description
PCI Express Root Port x	Enabled / Disabled	Controls the PCI Express Root Port
Connection Type	Built-in / Slot	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clrear. Slot: this rootport connects to used-sccessible slot. SlotImplemented but will be set.
ASPM	Disabled / L0s / L1 / LosL1 / Auto	Set the ASPM level
L1 Substates	DFisabled / L1.1 / L1.1 & L1.2	PCI Express L1 Substates
Hot Plug	Enabled / Disabled	PCI Express Hot Plug Enable / Disable
PCle Speed	Auto / Gen1 / Gen2 / Gen3	Configure PCle Speed

4.4.2.2 SATA Configuration

Menu Item	Options	Description

SATA Controller(s)	Enabled / Disabled	Enable/Disable SATA Devices
SATA Test Mode	Enabled / Disabled	Test Mode Enable / Disable (Loop Back)
Port x	Enabled / Disabled	Enable / Disable SATA Port
Hot Plug	Enabled / Disabled	Designate this port as Hot Pluggable

4.4.2.3 USB Configuration

Menu Item	Options	Description
xHCI Compliance Mode	Enable / Disable	Option to Enable Compliance Mode. Default is Disabled.
USB3 Link Speed Selection	GEN1 / GEN2	Select USB3 Link Speed as GEN1 or GEN2

4.4.2.4 Security Configuration

Menu Item	Options	Description
RTC Memory Lock	Enabled / Disabled	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM
BIOS Lock	Enabled / Disabled	Enable / Disable the PCH BIOS Lock Enable feature. Required Enabled to ensure SMM protection of flash
Force unlock on all GPIO pads	Enabled / Disabled	If Enabled BIOS will force all GPIO pads to be in unlocked state

4.4.2.5 HD Audio Configuration

Menu Item	Options	Description
HD Audio	Enabled / Disabled	Control Detection of the HD-Audio device. When enabled, following menu items will appear
Audio DSP	Enabled / Disabled	Enables/Disables Audio DSP
Audio Link Mode	HD Audio Link SSP (I2S) SoundWire Advanced Link Config	Select link mode: 1) HDA-Link [SDIO-1], DMIC[0-1] 2) SSP[0-5], DMIC[0-1] 3) SNDW[1-4] 4) Advanced will allow to enable each interface separately
HDA-Link Codec Select	Platform Onboard External Kit	Selects whether Platform Onboard Codec (single Verb Table installed) or External Codec Kit (multiple Verb Tables installed) will be used
HD Audio Advanced Configuration	See submenu	HD Audio Subystem Advanced Configuration Settings

4.4.2.5.1 HD Audio Advanced Configuration

Menu Item	Options	Description
iDisplay Audio Disconnect	Enabled / Disabled	Disconnects SDI2 signal to hide (disable) iDisplay Audio Codec
Codec Sx Wake Capability	Enabled / Disabled	Capability to detect wake initiated by a codec in Sx (e.g. by modem codec)
PME Enable	Enabled / Disabled	Enables PME wake of HD Audio controller during POST
HD Link Frequency	6 MHz 12 MHz 24 MHz	Selects HD Audio Link frequency. Applicable only if HAD codec supports selected frequency
iDisplay Audio Link Frequency	48 MHz 96 MHz	Selects iDisplay Link frequency
iDisplay Audio Link T-Mode	2T / 4T / 8T / 16T	Indicate whether SDI is operating in 1T, 2T (CNL) or 2T, 4T, 8T mode (ICL)
Autonomous Clock Stop SNDW #x	Enabled / Disabled	Enable / Disable Autonomous Clock Stop for SoundWire LINK number x
Data on Active Interval Select SNDW #x	3 / 4 / 5 / 6	Data on Active Interval Select Clock Periods for SoundWire LINK number x
Data on Delay Select SNDW #x	2 / 3	Data on Delay Select Clock Periods for SoundWire LINK number x

4.4.2.6 SerialIo Configuration

Menu Item	Options	Description
I2C3 Controller	Enabled / Disabled	The following devices depend on each other: I2C0 and I2C1-2-3
SPI1 Controller	Enabled / Disabled	The following devices depend on each other: UART0, UART1 and SPI0-1
SPI2 Controller	Enabled / Disabled	Depends on: Thermal Subsystem in PCI mode. SPI2 will be disabled if PSE SPI0, PWM or TGPIO are enabled.
UART0 Controller	Enabled / Disabled	The following devices depend on each other: UART0, UART1 and SPI0-1 UART 0 (00:30:00) cannot be disabled when: Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when: I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)

UART1 Controller	Enabled / Disabled / Comm. Port (COM)	The following devices depend on each other: UART0, UART1 and SPI0-1
GPIO IRQ Route	IRQ14 / IRQ15	Route all GPIOs to one of the IRQ
Serial IO I2Cx Settings		Configure SerialIO Controller --> Set specific parameters
Serial IO SPIx Settings		Configure SerialIO Controller --> Set specific parameters
Serial IO UARTx Settings		Configure SerialIO Controller --> Set specific parameters
WITT/MITT I2C Test Device	Enabled / Disabled	Enable SIO I2C WITT Device and select which controller use it
WITT/MITT SPI Test Device	Enabled / Disabled	Enable SIO SPI WITT Device and select which controller use it
UART Test Device	Enabled / Disabled	Enable SIO UART Test Device and select which controller use it
LPSS Device D3 State	Enabled / Disabled	Enable / Disable the LPSS D3 before entering to OS
Additional Serial IO devices	Enabled / Disabled	When enabled, ACPI will report additional devices connected to Serial IO
SerilaIO timing parameters	Enabled / Disabled	Enables additional timing parameters for all SerialIO controllers. Defaults can be changed in each controller setting. Platform restart quired to apply changes.

4.4.2.7 SCS Configuration

Menu Item	Options	Description
eMMC 5.1 Controller	Enabled / Disabled	Enable or Disable SCS eMMC 5.1 Controller
eMMC 5.1 HS400 Mode	Enabled / Disabled	Enable or Disable SCS eMMC HS400 Mode
Enable HS400 software tuning	Enabled / Disabled	Software tuning should improve eMMC HS400 stabilit at the expense of boot time
Driver Strength	33 / 40 / 50 Ohm	Sets IO driver trength
SDCard 3.0 Controller	Enabled / Disabled	Enable or Disable SCS SDHC 3.0 Controller

4.4.2.8 PSE Configuration

Menu Item	Options	Description
PSE Controller	Enabled / Disabled	Enables/Disables Programmable Service Engine (PSE). When enabled, following menu items will appear
LOG OUTPUT OFFSET		Determine the PSE log output region offset in memory
LOG OUTPUT SIZE		Determine the PSE log output region size limitation in memory
Shell	Enabled / Disabled	Enables/Disables PSE Shell

Eclite	Enabled / Disabled	Enables/Disables PSE Eclite Service
CPU Temp Read	Enabled / Disabled	Enables/Disables PSE Eclite CPU Temp Read
OOB	Enabled / Disabled	Enables/Disables PSE OOB Service
WoL	Enabled / Disabled	Enables/Disables PSE GBE Wake On Lan
PSE Debug (JTAG/SWD) Enable	Enabled / Disabled	Enables/Disables PSE JTAG/SWD Debug
PSE JTAG/SWD PIN MUX	Enabled / Disabled	Enables/Disables PSE JTAG Pin Mux. Not allowed if Sci Pin Mux is enabled.
CAN0	None PSE owned Host owned	CAN0 has pin conflict with I2S0 and TGPIO 16-17
CAN1	None PSE owned Host owned	CAN0 has pin conflict with I2S0 and TGPIO 14-15
DMA0	None PSE owned Host owned	Select ownership for DMA0
DMA1	None PSE owned Host owned	Select ownership for DMA1
DMA2	None PSE owned Host owned	Select ownership for DMA2
GBE0	None PSE owned Host owned	Select ownership for GBE0
PSE GBE0 DLL Override	Enabled / Disabled	Enable/Disable PSE GBE0 DLL. To Enable this GBE0 must be Enabled.
PSE GBE0 Tx_Delay		Configure total number of delay elements in DLL slave. Default 16, Min 1, Max 63
GBE1	None PSE owned Host owned	Select ownership for GBE1
PSE GBE1 DLL Override	Enabled / Disabled	Enable/Disable PSE GBE1 DLL. To Enable this GBE1 must be Enabled.
PSE GBE1 Tx_Delay		Configure total number of delay elements in DLL slave. Default 16, Min 1, Max 63

GPIO/TGPIO 0 MUX SELECTION	LOWER / MID / TOP / All GPIO	Lower: TGPIO(0-19), GPIO(20-29) Lower: TGPIO(0-9, 20-29), GPIO(10-19) Lower: TGPIO(10-29)
GPIO/TGPIO 0 Pin Selection		Enables / Disables individual GPIO/TGPIO 0 pins
GPIO/TGPIO 1 MUX SELECTION	LOWER / MID / TOP / All GPIO	Lower: TGPIO(30-49), GPIO(50-59) Lower: TGPIO(30-39, 50-59), GPIO(40-49) Lower: TGPIO(40-59)
GPIO/TGPIO 1 Pin Selection		Enables / Disables individual GPIO/TGPIO 1 pins
List of PSE peripherals that can generate interrupts	Enabled / Disabled	Enabled = Interrupt set to SB mode; Disabled = MSI mode
DMA Test	Enabled / Disabled	Enables / Disables DMA test Device

4.4.2.9 TSN GBE Configuration

Menu Item	Options	Description
PCH TSN LAN Controller	Enabled / Disabled	Enable/Disable Time Sensitive Network (TSN) LAN
PCH TSN GBE Multi-Vc	Enabled / Disabled	Enable/Disable TSN Multi Virtual Channels
PCH TSN GBE SGMII Support	Enabled / Disabled	Enable/Disable SGMII mode for PCH TSN GBE. Ports in SGMII mode with the same PLL common lane must use the same link speed. SATA or UFS may need to be disabled if TSN port is using the same PLL common lane. Please make sure IFWI has proper straps set for SGMII. Make sure Flex IO Lane Assignment is not NONE
PCH TSN Link Speed	24MHz 2.5Gbps 24MHz 1Gbps 38.4MHz 2.5Gbps 38.4MHz 1bps	PCH TSN Link Speed configuration
PCH TSN GBE x Multi-Vc	Enabled / Disabled	Enable/Disable TSN Multi Virtual Channels. TSN GBE x must be host owned.
PCH TSN GBE x SGMII Support	Enabled / Disabled	Enable/Disable SGMII mode for PCH TSN GBE x. Ports in SGMII mode with the same PLL common lane must use the same link speed. UFS will need to be disabled as this TSN port uses the same PLL common lane. Please make sure IFWI has proper straps set for SGMII. Make sure Flex IO Lane Assignment is not NONE
PCH TSN GBE x Link Speed	24MHz 2.5Gbps 24MHz 1Gbps	PCH TSN GBE x Link Speed configuration

	38.4MHz 2.5Gbps 38.4MHz 1bps

4.5 Security menu

Menu Item	Options	Description
Administrator Password		Set Administrator Password
User Password		Set User Password
List of available storage units		HDD Security Configuration for selected drive --> Set HDD User Password
Secure Boot	See submenu	Secure Boot configuration

4.5.1 Secure Boot submenu

Menu Item	Options	
Secure Boot	Enabled / Disabled	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and System is in User Mode. The mode change requires platform reset.
Secure Boot Mode	Standard / Custom	Secure Boot Mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.
Restore Factory Keys		Force system to User Mode. Install factory default Secure Boot key databases.
Reset To Setup Mode		Delete all Secure Boot key databases from NVRAM
Key management	See submenu	Enable expert users to modify Secure Boot Policy variables without full authentication.

4.5.1.1 Key Management submenu

Menu Item	Options	
Factory Key Provision	Enabled / Disabled	Install factory default Secure Boot keys after the platform reset and while the system is in Setup mode
Restore Factory Keys		Force System to User Mode. Install factory default Secure Boot key databases
Reset To Setup Mode		Delete all Secure Boot key databases from NVRAM
Enroll Efi Image	*File System Image*	Allow the image to run in Secure Boot mode. Enrol SHA256 Hash certificate of a PE Image into Authorized Signature Database (db)
Remove ‘UEFI CA’ from DB		Device Guard ready system must not list ‘Microsoft UEFI CA’ Certificate in Authorized Signature database (db)

Restore DB defaults		Restore DB variable to factory defaults
Platform key (PK) Key Exchange Keys Authorized Signatures Forbidden Signatures Authorized Timestamps OS Recovery Signatures	Set New Var Append Key	Enrol factory Defaults or load certificates from a file: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHAxxx 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256), Key Source: Factory, External, Mixed

4.6 Boot menu

Menu Item	Options	Description
Setup Prompt Timeout	0 .. 65535	Number of seconds to wait for setup activation key. 655535 means indefinite waiting.
Bootup NumLock State	On / Off	Select the keyboard NumLock state
Quiet Boot	Enabled / Disabled	Enables or disables Quiet Boot option
Fast Boot	Enabled / Disabled	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.
SATA Support	Last Boot SATA Devices Only All SATA Devices	If Last Boot SATA Devices Only, only last boot SATA device will be available in Post. If All SATA Devices, all SATA devices will be available in OS and Post.
NVMe Support	Enabled / Disabled	If Disabled, NVMe device will be skipped
USB Support	Disabled Full Initial Partial Initial	If Disabled, all USB devices will NOT be available until after OS boot. If Partial Initial, USB Mass Storage and specific USB port/device will NOT be available before OS boot. If Enabled, all USB devices will be available in OS and Post.
PS2 Devices Support	Enabled / Disabled	If Disabled, PS2 devices will be skipped
Network Stack Driver Support	Enabled / Disabled	If Disabled, Network Stack Driver will be skipped
Redirection Support	Enabled / Disabled	If Disabled, Redirection function will be disabled
Boot Option #1 Boot Option #2 Boot Option #3 Boot Option #4 Boot Option #5 Boot Option #6 Boot Option #7 Boot Option #8 Boot Option #9	Hard Disk0 Hard Disk1 eMMC CD/DVD SD USB Device Network Other Device Disabled	Select the system boot order
UEFI EMMC Drive BBS Priorities		Specifies the Boot Device Priority sequence from available UEFI EMMC Drivers
UEFI SD Drive BBS Priorities		Specifies the Boot Device Priority sequence from available UEFI SD Drivers

4.7 Save & Exit menu

Menu Item	Options	Description
Save Changes and Exit		Exit system setup after saving the changes.
Discard Changes and Exit		Exit system setup without saving any changes.
Save Changes and Reset		Reset the system after saving the changes.
Discard Changes and Reset		Reset the system without saving any changes.
Save Changes		Save the changes done so far to any of the setup options.
Discard Changes		Discard the changes done so far to any of the setup options.
Restore Defaults		Restore/Load Default values for all the setup options
Save as User Defaults		Save the changes done so far as User Defaults
Restore User Defaults		Restore the User Defaults to all the setup options
List of EFI boot managers available		Boot override to selected boot manager

Chapter 5.
Appendices

- Thermal Design

5.1 Thermal Design

Highly integrated modules, like this product, offer very high performance within small dimensions. On the other hand, the miniaturization of ICs and the high operating frequencies of the processors lead to high heat generation that must be dissipated in order to maintain the CPU within its allowed temperature range.

The operating temperature specified in the Technical Features of this product indicates the temperature range in which any and all parts of the heat spreader / heat sink must remain, in order for SECO to guarantee functionality. Hence, these numbers do not necessarily indicate the suitable environmental temperature.

The heat spreader is not intended to be a guaranteed standalone cooling system, but should be used only as a supplemental means of transferring heat to another dissipation system (i.e. heat sinks, fans, heat pipes etc).

It is the customer's responsibility to design and apply an application-dependent cooling system, capable of ensuring that the heat spreader / heat sink temperature remain within the indicated range of the module.

It is an absolute requirement that the customer, after thorough evaluation of the processor's workload in the actual system application, the system enclosure and consequent air flow/Thermal analysis, accurately study and develop a suitable cooling solution for the assembled system.

SECO can provide specific heatspreaders and heatsinks for this module, but please remember that their use must be evaluated accurately inside the final system, and that they should be used only as a part of a more comprehensive ad-hoc cooling solutions.

Ordering Code	Description
RC93-DISS-1-SKUS1-4-PK	SMARC HEAT SPREADER: HALLEY Heat Spreader (PASSIVE), SKUS1-4 - Packaged
RC93-DISS-1-SKUS5-12-PK	SMARC HEAT SPREADER: HALLEY Heat Spreader (PASSIVE), SKUS5-12 - Packaged
RC93-DISS-2-SKUS1-4-PK	SMARC HEAT SINK: HALLEY Heat Sink (PASSIVE), SKUS1-4 – Packaged
RC93-DISS-2-SKUS5-12-PK	SMARC HEAT SINK: HALLEY Heat Sink (PASSIVE), SKUS5-12 – Packaged

Warning!

The thermal solutions available with SECO boards are tested in the commercial temperature range (0-60°C), without housing and inside climatic chamber. Therefore, the customer is suggested to study, develop and validate the cooling solution for his system, considering ambient temperature, processor's workload, utilisation scenarios, enclosures, air flow and so on.

In particular, the heatspreader is not intended to be a cooling system by itself, but only as the standard means for transferring heat to cooler, like heatsinks, cold plate, heat pipes and so on.

SECO S.p.A. - Via A. Grandi, 20
52100 Arezzo - ITALY
Ph: +39 0575 26979 - Fax: +39 0575 350210
www.seco.com