USER GUIDE

SMARC-sXEL

Doc. User Guide Rev. 1.7

Doc. ID: 1068-8367

www.kontron.com

kontron
The Power of IoT

This page has been intentionally left blank

SMARC-SXEL - USER GUIDE

Disclaimer

Kontron would like to point out that the information contained in this user guide may be subject to alteration, particularly as a result of the constant upgrading of Kontron products. This document does not entail any guarantee on the part of Kontron with respect to technical processes described in the user guide or any product characteristics set out in the user guide. Kontron assumes no responsibility or liability for the use of the described product(s), conveys no license or title under any patent, copyright or mask work rights to these products and makes no representations or warranties that these products are free from patent, copyright or mask work right infringement unless otherwise specified. Applications that are described in this user guide are for illustration purposes only. Kontron makes no representation or warranty that such application will be suitable for the specified use without further testing or modification. Kontron expressly informs the user that this user guide only contains a general description of processes and instructions which may not be applicable in every individual case. In cases of doubt, please contact Kontron.

This user guide is protected by copyright. All rights are reserved by Kontron. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the express written permission of Kontron. Kontron points out that the information contained in this user guide is constantly being updated in line with the technical alterations and improvements made by Kontron to the products and thus this user guide only reflects the technical status of the products by Kontron at the time of publishing.

Brand and product names are trademarks or registered trademarks of their respective owners.

©2021 by Kontron S&T AG

Kontron Europe GmbH

Gutenbergstr. 2
85737 Ismaning, Germany
www.kontron.com

Intended Use

THIS DEVICE AND ASSOCIATED SOFTWARE ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE FOR THE OPERATION OF NUCLEAR FACILITIES, THE NAVIGATION, CONTROL OR COMMUNICATION SYSTEMS FOR AIRCRAFT OR OTHER TRANSPORTATION, AIR TRAFFIC CONTROL, LIFE SUPPORT OR LIFE SUSTAINING APPLICATIONS, WEAPONS SYSTEMS, OR ANY OTHER APPLICATION IN A HAZARDOUS ENVIRONMENT, OR REQUIRING FAIL-SAFE PERFORMANCE, OR IN WHICH THE FAILURE OF PRODUCTS COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE (COLLECTIVELY, "HIGH RISK APPLICATIONS").

You understand and agree that your use of Kontron devices as a component in High Risk Applications is entirely at your risk. To minimize the risks associated with your products and applications, you should provide adequate design and operating safeguards. You are solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning your products. You are responsible to ensure that your systems (and any Kontron hardware or software components incorporated in your systems) meet all applicable requirements. Unless otherwise stated in the product documentation, the Kontron device is not provided with error-tolerance capabilities and cannot therefore be deemed as being engineered, manufactured or setup to be compliant for implementation or for resale as device in High Risk Applications. All application and safety related information in this document (including application descriptions, suggested safety measures, suggested Kontron products, and other materials) is provided for reference only.

NOTICE

You find the most recent version of the “General Safety Instructions“ online in the download area of this product.

NOTICE

This product is not suited for storage or operation in corrosive environments, in particular under exposure to sulfur and chlorine and their compounds. For information on how to harden electronics and mechanics against these stress conditions, contact Kontron Support.

Revision History

Revision	Brief Description of Changes	Date of Issue	Author/ Editor
1.0	Initial version	2021-Sept-17	CW
1.1	Updates to Chapters 8.2: Watch Dog, 8.3.1: Suspend States, 8.3.3: Power Management Signals	2021-Oct-04	CW
1.2	Block Diagram DDI2 is HDMI, Table 12 DDI2 is HDMI only and restricted to HDMI 1.4.	2022-Sept-19	CW
1.3	Removed AC Coupled off Module for pins (92, 93, 95, 96, 97, 99, 101, 102)	2023-Sept-14	CW
1.4	Updated the Eth PHY in Tabel 1 to 1 GbE and rephrased the text in Chapter 6.8 Ethernet.	2023-Oct-04	CW
1.5	Update to new carrier part number in Table 2	2024-Feb-14	CW
1.6	Updated Table 30 and Table 31, and added the new Kontron Logo.	2024-May-13	CW
1.7	Updated Chapter 6.1 Processor Support with DTR information and added the new Kontron Logo.	2024-May-24	CW

Terms and Conditions

Kontron warrants products in accordance with defined regional warranty periods. For more information about warranty compliance and conformity, and the warranty period in your region, visit https://www.kontron.com/terms-and-conditions.

Kontron sells products worldwide and declares regional General Terms & Conditions of Sale, and Purchase Order Terms & Conditions. Visit https://www.kontron.com/terms-and-conditions.

For contact information, refer to the corporate offices contact information on the last page of this user guide or visit our website CONTACT US.

Customer Support

Find Kontron contacts by visiting: https://www.kontron.com/en/support-and-services.

Customer Service

As a trusted technology innovator and global solutions provider, Kontron extends its embedded market strengths into a services portfolio allowing companies to break the barriers of traditional product lifecycles. Proven product expertise coupled with collaborative and highly-experienced support enables Kontron to provide exceptional peace of mind to build and maintain successful products.

For more details on Kontron's service offerings such as: enhanced repair services, extended warranty, Kontron training academy, and more visit https://www.kontron.com/en/support-and-services.

Customer Comments

If you have any difficulties using this user guide, discover an error, or just want to provide some feedback, contact Kontron support. Detail any errors you find. We will correct the errors or problems as soon as possible and post the revised user guide on our website.

Symbols

The following symbols may be used in this user guide

⚠DANGER	DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.
⚠WARNING	WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.
NOTICE	NOTICE indicates a property damage message.
⚠CAUTION	CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.
	Electric Shock! This symbol and title warn of hazards due to electrical shocks (> 60 V) when touching products or parts of products. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material.
	ESD Sensitive Device! This symbol and title informs that the electronic boards and their components are sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.
	HOT Surface! Do NOT touch! Allow to cool before servicing.
	Laser! This symbol informs of the risk of exposure to laser beam and light emitting devices (LEDs) from an electrical device. Eye protection per manufacturer notice shall review before servicing.
	This symbol indicates general information about the product and the user guide. This symbol also indicates detail information about the specific product configuration.
	This symbol precedes helpful hints and tips for daily use.

For Your Safety

Your new Kontron product was developed and tested carefully to provide all features necessary to ensure its compliance with electrical safety requirements. It was also designed for a long fault-free life. However, the life expectancy of your product can be drastically reduced by improper treatment during unpacking and installation. Therefore, in the interest of your own safety and of the correct operation of your new Kontron product, you are requested to conform with the following guidelines.

High Voltage Safety Instructions

As a precaution and in case of danger, the power connector must be easily accessible. The power connector is the product's main disconnect device.

⚠CAUTION

Warning

All operations on this product must be carried out by sufficiently skilled personnel only.

⚠CAUTION

Electric Shock!

Before installing a non hot-swappable Kontron product into a system always ensure that your mains power is switched off. This also applies to the installation of piggybacks. Serious electrical shock hazards can exist during all installation, repair, and maintenance operations on this product. Therefore, always unplug the power cable and any other cables which provide external voltages before performing any work on this product.

Earth ground connection to vehicle's chassis or a central grounding point shall remain connected. The earth ground cable shall be the last cable to be disconnected or the first cable to be connected when performing installation or removal procedures on this product.

Special Handling and Unpacking Instruction

NOTICE

ESD Sensitive Device!

Electronic boards and their components are sensitive to static electricity. Therefore, care must be taken during all handling operations and inspections of this product, in order to ensure product integrity at all times.

⚠CAUTION

Handling and operation of the product is permitted only for trained personnel within a work place that is access controlled. Follow the "General Safety Instructions" supplied with the system.

Do not handle this product out of its protective enclosure while it is not used for operational purposes unless it is otherwise protected.

Whenever possible, unpack or pack this product only at EOS/ESD safe work stations. Where a safe work station is not guaranteed, it is important for the user to be electrically discharged before touching the product with his/her hands or tools. This is most easily done by touching a metal part of your system housing.

It is particularly important to observe standard anti-static precautions when changing piggybacks, ROM devices, jumper settings etc. If the product contains batteries for RTC or memory backup, ensure that the product is not placed on conductive surfaces, including anti-static plastics or sponges. They can cause short circuits and damage the batteries or conductive circuits on the product.

Lithium Battery Precautions

If your product is equipped with a lithium battery, take the following precautions when replacing the battery.

⚠CAUTION

CAUTION: Risk of Explosion if the lithium battery is replaced by an incorrect type. Dispose of used lithium batteries according to the Instructions.

ATTENTION: Risque d'explosion si la pile au lithium est remplacée par une pile de type incorrect. Éliminez les piles au lithium usagées conformément aux instructions.

General Instructions on Usage

In order to maintain Kontron's product warranty, this product must not be altered or modified in any way. Changes or modifications to the product, that are not explicitly approved by Kontron and described in this user guide or received from Kontron Support as a special handling instruction, will void your warranty.

This product should only be installed in or connected to systems that fulfill all necessary technical and specific environmental requirements. This also applies to the operational temperature range of the specific board version that must not be exceeded. If batteries are present, their temperature restrictions must be taken into account.

In performing all necessary installation and application operations, only follow the instructions supplied by the present user guide.

Keep all the original packaging material for future storage or warranty shipments. If it is necessary to store or ship the product, then re-pack it in the same manner as it was delivered.

Special care is necessary when handling or unpacking the product. See Special Handling and Unpacking Instruction.

Quality and Environmental Management

Kontron aims to deliver reliable high-end products designed and built for quality, and aims to complying with environmental laws, regulations, and other environmentally oriented requirements. For more information regarding Kontron's quality and environmental responsibilities, visit http://www.kontron.com/about-kontron/corporate-responsibility/quality-management.

Disposal and Recycling

Kontron's products are manufactured to satisfy environmental protection requirements where possible. Many of the components used are capable of being recycled. Final disposal of this product after its service life must be accomplished in accordance with applicable country, state, or local laws or regulations.

WEEE Compliance

The Waste Electrical and Electronic Equipment (WEEE) Directive aims to:

- Reduce waste arising from electrical and electronic equipment (EEE)
- Make producers of EEE responsible for the environmental impact of their products, especially when the product become waste
- Encourage separate collection and subsequent treatment, reuse, recovery, recycling and sound environmental disposal of EEE
- Improve the environmental performance of all those involved during the lifecycle of EEE

Environmental protection is a high priority with Kontron.

Kontron follows the WEEE directive

Table of Contents

Symbols **6**
For Your Safety **7**
High Voltage Safety Instructions 7
Special Handling and Unpacking Instruction 7
Lithium Battery Precautions 8
General Instructions on Usage **8**
Quality and Environmental Management **8**
Disposal and Recycling 8
WEEE Compliance 8
Table of Contents **9**
List of Tables **10**
List of Figures **11**
1/ Introduction **13**
2/ General Safety Instructions **14**
2.1. Electrostatic Discharge (ESD) 15
2.1.1. Grounding Methods 15
3/ Description **16**
3.1. SMARC™ Modules 16
3.2. SMARC-sXEL Module 16
3.3. Variants 17
4/ System Specification **18**
4.1. Functional Block Diagram 18
4.2. Top Side Features 19
4.3. Rear Side Features 19
4.4. Component Main Data Specification 20
4.5. Mechanical Specification 21
4.5.1. Mechanical Drawings 21
4.6. Thermal Management Specification 23
4.6.1. Heatspreader 23
4.7. Environmental Specification 25
4.8. Compliance 26
4.8.1. MTBF 27
4.9. Power Specification 28
5/ Module and Connectors **29**
5.1. Connectors Location 29
5.2. SMARC Connector 29
5.3. 3-pin Fan Connector 29
6/ Features and Interfaces **30**
6.1. Processor Support 30
6.2. System Memory Support 31
6.3. Graphics (LVDS, eDP, DP++, HDMI) 31
6.4. HD Audio Interfaces 32
6.5. HSIO Overview 32
6.6. USB 32
6.6.1. USB 2.0 Client Mode 33
6.7. PCIe 3.0 33
6.8. Ethernet 33

6.8.1. SGMII via SERDES (option) 34
6.8.2. Link and Activity LEDs 34
6.9. SATA 3.0 34
6.10. CAN Bus Interfaces 35
6.11. Eeep 35
6.12. eMMC Flash Memory (option) 35
6.13. I2C Bus Support 35
6.14. Kontron CPLD 35
6.15. RTC 36
6.16. SDIO 36
6.17. SPI Interfaces 37
6.17.1. SPI Boot Flash Chip 37
6.18. TPM 2.0 37
6.19. UART Interfaces 38
7/ Pin Definitions 39
7.1. Smart Connector 39
7.1.1. Pinout of SMARC Connector (Top Side) 40
7.1.2. Pinout of SMARC Connector (Bottom Side) 51
8/ Configuration 66
8.1. Boot Select 66
8.1.1. Booting the SPI Flash 66
8.2. Watch Dog 67
8.2.1. Watchdog Timer Signal 67
8.3. Power Management 67
8.3.1. Suspend States 67
8.3.2. Power Button (POWER_BTN#) 68
8.3.3. Power Management Signals 68
9/ uEFI BIOS 69
9.1. Starting the uEFI BIOS 69
9.2. Navigating the uEFI BIOS 69
9.3. Setup Menus 70
9.4. Main Setup Menu 70
9.5. Advanced Setup Menu 72
9.6. Chipset 86
9.7. Security Setup Menu 100
9.7.1. Remember the Password 101
9.8. Boot Setup Menu 102
9.9. Save and Exit Setup Menu 103
10/ Technical Support 105
10.1. Returning Defective Merchandise 105
11/ Warranty 106
11.1. Limitation/Exemption from Warranty Obligation 106
List of Acronyms 107
About Kontron 108

List of Tables

Table 1: SMARC-sXEL Product Variants 17
Table 2: SMARC-sXEL Accessories 17

Table 3: Component Main Data....20
Table 4: Environmental Conditions....25
Table 5: Compliance CE....26
Table 6: Country Compliance....26
Table 7: MTBF....27
Table 8: Power Supply Voltage Requirements....28
Table 9: Fan Connector....29
Table 10: Supported Processors....30
Table 11: LPDDR4 Memory Options....31
Table 12: Digital Display Interfaces (DDI)....31
Table 13: HD Audio....32
Table 14: I2S Audio....32
Table 15: HSIO Lane Overview....32
Table 16: USB 3.1 Ports....32
Table 17: USB 2.0 Ports....33
Table 18: PCIe Lanes....33
Table 19: Ethernet Ports....34
Table 20: GBE LEDs....34
Table 21: SATA Ports....34
Table 22: CAN Bus....35
Table 23: eMMC Flash Memory....35
Table 24: Kontron CPLD....36
Table 25: SDIO Interface....36
Table 26: Supported SPI Boot Flash Types....37
Table 27: UART Serial Port....38
Table 28: Connector Definitions....39
Table 29: SMARC Pinout Legend....40
Table 30: SMARC 2.1 Specification Pinout (Top side)....40
Table 31: SMARC 2.1 Specification Pinout (bottom side)....51
Table 32: Boot Select....66
Table 33: Dual Staged Watchdog Timer- Time-Out Events....67
Table 34: Power Management Pins....68
Table 35: Navigation Hot Keys Available in the Legend Bar....69
Table 36: Main Setup Menu Sub-screens and Functions....70
Table 37: Advanced Setup Menu Sub-screens and Functions....72
Table 38: Chipset Setup Menu Sub-screens and Functions....86
Table 39: Security Setup Menu Sub-screens and Functions....100
Table 40: Boot Setup Menu Sub-screens and Functions....102
Table 41: Save and Exit Setup Menu Sub-screens and Functions....103
Table 42: List of Acronyms....107

List of Figures

Figure 1: SMARC-sXEL Module....16
Figure 2: Block Diagram....18
Figure 3: Top Side....19
Figure 4: Rear Side....19
Figure 5: Dimensions of SMARC-sXEL - Industrial....21
Figure 6: Thickness from the Side View - Industrial....21
Figure 7: Dimensions of SMARC-sXEL - Commercial....22
Figure 8: Thickness from the Side View, Commercial....22
Figure 9: Temperature Sensors....23
Figure 10: Heatspreader as Cooling Solution....24
Figure 11: Heatspreader Height for Industrial Variants....24
Figure 12: Heatspreader Height for Commercial Variants....25
Figure 13: Connectors (top side)....29

Figure 14: 3-Pin Power Connector 29
Figure 15: SMARC Connector 314-Pin 40
Figure 16: Main Setup Menu 70
Figure 17: Advanced Setup Menu 72
Figure 18: Chipset Setup Menu 86
Figure 19. Security Setup Menu 100
Figure 20: Boot Setup Menu 102
Figure 21: Save and Exit Setup Menu 103

1/ Introduction

This user guide describes the Smart Mobility Architecture (SMARC) SMARC-sXEL module, known as module within this user guide and designed for use with a carrier board.

The use of this user guide implies a basic knowledge of PC hard- and software. This user guide is focused on describing the special features and is not intended to be a standard PC textbook.

New users are recommended to observe the instruction in the user guide before connecting the power.

All configuration and setup of the module is either done automatically or manually by the user via the BIOS setup menus.

Latest revision of this user guide, datasheet, BIOS, drivers and BSP's (Board Support Packages) can be downloaded from Kontron Web Page.

2/ General Safety Instructions

Please read this passage carefully and take careful note of the instructions, which have been compiled for your safety and to ensure to apply in accordance with intended regulations. If the following general safety instructions are not observed, it could lead to injuries to the operator and/or damage of the product; in cases of non-observance of the instructions Kontron Europe is exempt from accident liability, this also applies during the warranty period.

The product has been built and tested according to the basic safety requirements for low voltage (LVD) applications and has left the manufacturer in safety-related, flawless condition. To maintain this condition and to also ensure safe operation, the operator must not only observe the correct operating conditions for the product but also the following general safety instructions:

- The product must be used as specified in the product documentation, in which the instructions for safety for the product and for the operator are described. These contain guidelines for setting up, installation and assembly, maintenance, transport or storage.
- The on-site electrical installation must meet the requirements of the country's specific local regulations.
- If a power cable comes with the product, only this cable should be used. Do not use an extension cable to connect the product.
- To guarantee that sufficient air circulation is available to cool the product, please ensure that the ventilation openings are not covered or blocked. If a filter mat is provided, this should be cleaned regularly. Do not place the product close to heat sources or damp places. Make sure the product is well ventilated.
- Only connect the product to an external power supply providing the voltage type (AC or DC) and the input power (max. current) specified on the Kontron Product Label and meeting the requirements of the Limited Power Source (LPS) and Power Source (PS2) of UL/IEC 62368-1.
- Only products or parts that meet the requirements for Power Source (PS1) of UL/IEC 62368-1 may be connected to the product's available interfaces (I/O).
- Before opening the product, make sure that the product is disconnected from the mains.
- Switching off the product by its power button does not disconnect it from the mains. Complete disconnection is only possible if the power cable is removed from the wall plug or from the product. Ensure that there is free and easy access to enable disconnection.
- The product may only be opened for the insertion or removal of add-on cards (depending on the configuration of the product). This may only be carried out by qualified operators.
- If extensions are being carried out, the following must be observed:
- all effective legal regulations and all technical data are adhered to
- the power consumption of any add-on card does not exceed the specified limitations
- the current consumption of the product does not exceed the value stated on the product label.
- Only original accessories that have been approved by Kontron Europe can be used.
- Please note: safe operation is no longer possible when any of the following applies:
    - the product has visible damages or
    - the product is no longer functioning
      In this case the product must be switched off and it must be ensured that the product can no longer be operated.
- Handling and operation of the product is permitted only for trained personnel within a work place that is access controlled.
- CAUTION: Risk of explosion if the battery is replaced incorrectly (short-circuited, reverse-poled, wrong battery type). Dispose of used batteries according to the manufacturer's instructions.
- This product is not suitable for use in locations where children are likely to be present

Additional Safety Instructions for DC Power Supply Circuits

- To guarantee safe operation, please observe that:
    - the external DC power supply must meet the criteria for LPS and PS2 (UL/IEC 62368-1)

- no cables or parts without insulation in electrical circuits with dangerous voltage or power should be touched directly or indirectly
- a reliable protective earthing connection is provided
- a suitable, easily accessible disconnecting device is used in the application (e.g. overcurrent protective device), if the product itself is not disconnectable
- a disconnect device, if provided in or as part of the product, shall disconnect both poles simultaneously
- interconnecting power circuits of different products cause no electrical hazards

- A sufficient dimensioning of the power cable wires must be selected – according to the maximum electrical specifications on the product label – as stipulated by EN62368-1 or VDE0100 or EN60204 or UL61010-1 regulations.

2.1. Electrostatic Discharge (ESD)

A sudden discharge of electrostatic electricity can destroy static-sensitive devices or micro-circuitry.

Therefore, proper packaging and grounding techniques are necessary precautions to prevent damage. Always take the following precautions:

1. Transport ESD sensitive parts in ESD safe containers such as boxes or bags, until they arrive at an ESD safe workplace.
2. Always be properly grounded when touching sensitive components, or assembly.
3. Store ESD sensitive components in protective packaging or on antistatic mats.

2.1.1. Grounding Methods

By adhering to the guidelines below, electrostatic damage to the product can be avoided:

1. Cover workstations with approved antistatic material/mat. Always wear a wrist strap connected to workplace or heel straps.
2. Use properly grounded tools and equipment such as field service tools that are conductive.
3. Always handle ESD sensitive components by their edge or by their casing.
4. Avoid contact with pins, leads, or circuitry.
5. Switch off power and input signals before inserting and removing connectors or connecting test equipment.
6. Keep work area free of non-conductive materials such as ordinary plastic assembly aids and Styrofoam.

3/ Description

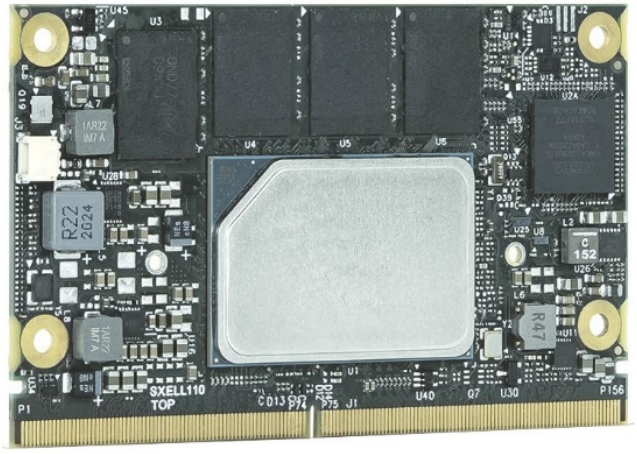
3.1. SMARC™ Modules

The SMARC™ standard was developed especially for new modules with SOC processors. Modules with this interfaces are characterized by the extremely flat form factor. The SMARC or MXM 3.0 connector comes with 314 pins and a construction height of just 4.3 millimeters. The connector is also available in a shock- and vibration resistant version for rough environmental conditions. Furthermore, the standard integrates dedicated interfaces for the latest processors. OEMs profit from minimized design effort and low Bill of Material (BoM) costs. SMARC™ defines two different module sizes in order to offer a high level of flexibility regarding different mechanical requirements.

3.2. SMARC-sXEL Module

The SMARC-sXEL is a SMARC half-size module using the Intel® Atom®/Pentium®/Celeron® 6xxx processor family and based on the latest SMARC 2.1 specification.

Figure 1: SMARC-sXEL Module



General features are:

- Up to 16 GByte LPDDR4 memory down with in-band ECC support
- 2x USB 3.0/2.0
- 4x USB 2.0 Host
- 2x LAN option or standard
- 1x SATA 6 Gb/s
- Up to 128 GByte eMMC (MLC) or option for up to 64 GByte eMMC (pSLC)
- Up to 4 PCIe x1 or opt. 3xPCIe & 1x SERDES
- Panel signal:
  - 1x HDMI (on request DP)
  - 1x DP++
  - 1x LVDS dual channel (on request eDP)
- 3x Serial interfaces (2x RX/TX only)
- 1x HD Audio and I2S Audio
- 2x I2C interfaces
- 2x SPI
- 14x GPIO
- Special Features: TPM and Industrial temperature grade versions

3.3. Variants

The SMARC-sXEL module variants are:

Table 1: SMARC-sXEL Product Variants

Product Number	SoC	Memory	Flash	Eth Phy	Display	SERDES	Op Temp.
51016-0432-J2-4	J6426	4 GByte	32 GByte	2x 1 GbE	LVDS, HDMI, DP++	No	0°C to 60°C
51016-0416-N1-2	N6211	4 GByte	16 GByte	2x 1 GbE	LVDS, HDMI, DP++	No	0°C to 60°C
51017-0416-R1-2	X6212RE	4 GByte	16 GByte	2x 1 GbE	LVDS, HDMI, DP++	No	-40°C to 85°C
51017-0432-R1-4	X6414RE	4 GByte	32 GByte	2x 1 GbE	LVDS, HDMI, DP++	No	-40°C to 85°C
51017-0832-R2-4	X6425RE	8 GByte	32 GByte	2x 1 GbE	LVDS, HDMI, DP++	No	-40°C to 85°C

The SMARC-sXEL accessories are:

Table 2: SMARC-sXEL Accessories

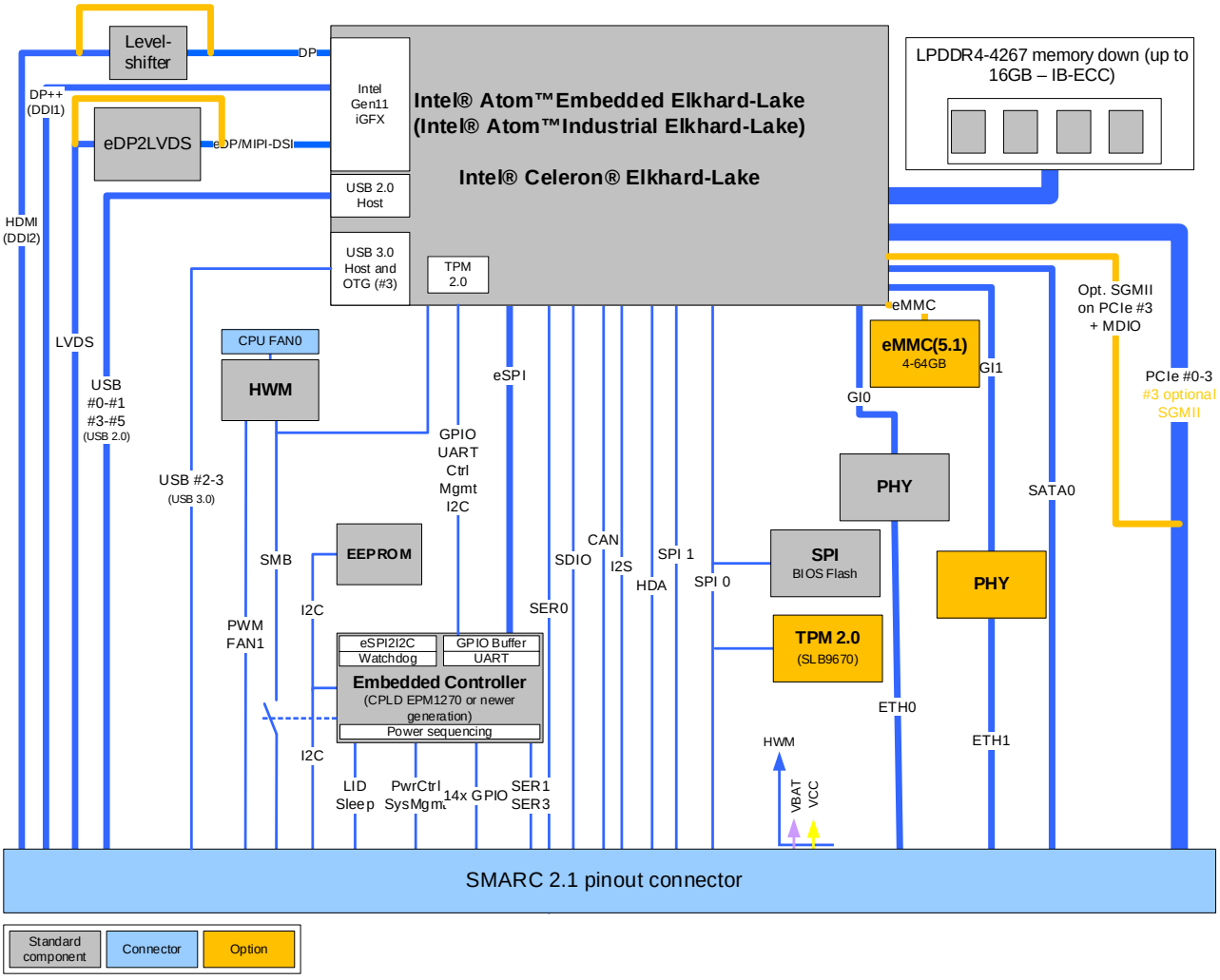
Part Number	Article	Description
Carrier		
51301-0000-00-0	SMARC Evaluation Carrier 2.1	SMARC Evaluation Carrier for SMARC modules according to the SMARC 2.1 standard (without SMARC module)
Cooling		
51016-0000-99-1	HSP SMARC-sXEL	Heatspreader for SMARC-sXEL (only for commercial temperature 51016-XXXXX-XX-X)
51017-0000-99-1	HSP SMARC-sXEL E2	Heatspreader for SMARC-sXEL (only for industrial temperature 51017-XXXXX-XX-X)
51099-0000-99-1	SMARC PASSIVE UNI COOLER (W/O HSP)	SMARC Passive Uni Cooler
Mounting		
51117-0000-00-0	SMARC MOUNTING KIT	Mounting Kit for SMARC modules

4/ System Specification

4.1. Functional Block Diagram

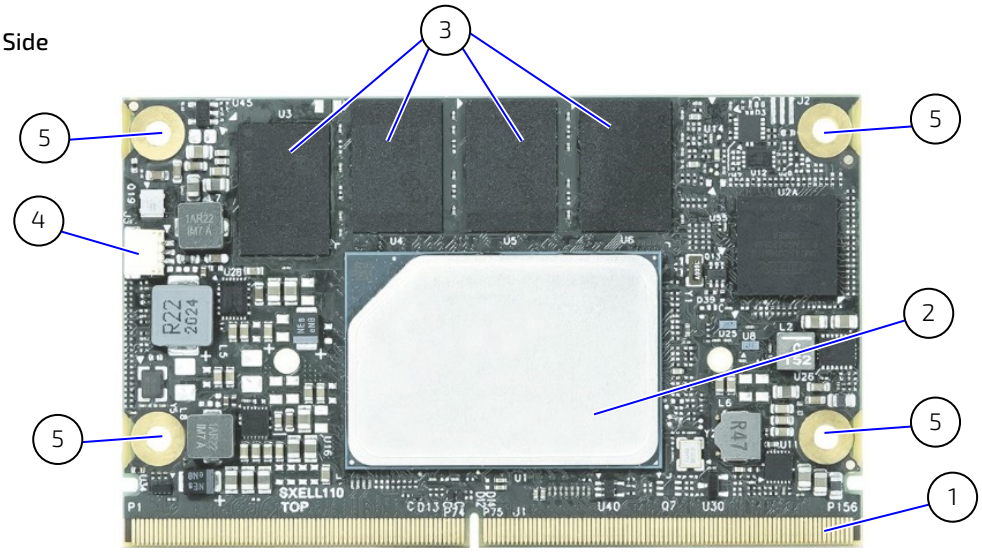
The block diagram shows all available SMARC-sXEL interfaces.

Figure 2: Block Diagram



4.2. Top Side Features

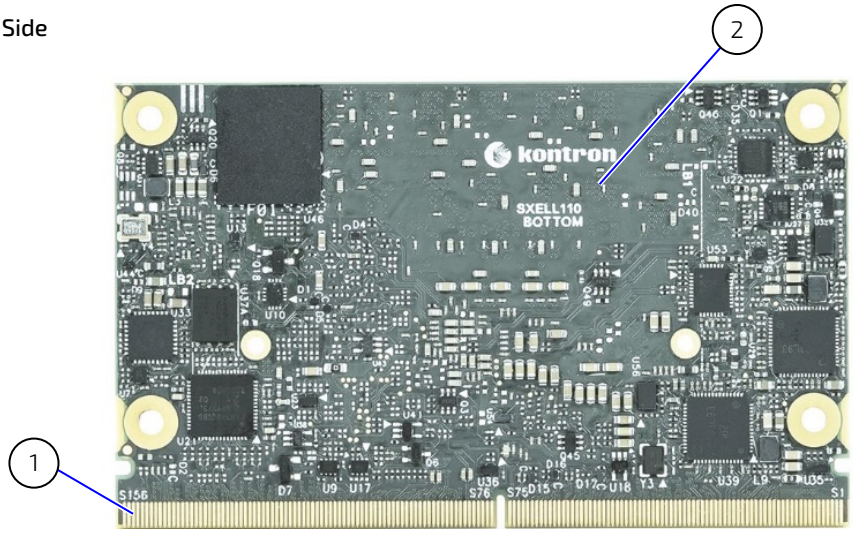
Figure 3: Top Side



1 SMARC 2.1 connector
2 Multi-Chip Package (MCP)
3 4x LPDDR memory down
4 3-pin fan connector
5 Mounting points

4.3. Rear Side Features

Figure 4: Rear Side



1 SMARC 2.1 connector
2 Product labelling

4.4. Component Main Data Specification

Table 3: Component Main Data

SMARC-sXEL	
Form factor	Short module form factor: 82 mm x 50 mm, max. thickness 6 mm
Processor	Intel® Atom®/Pentium®/Celeron® 6xxx processor family
Main Memory	Up to 16 GByte LPDDR4 memory down with in-band ECC support
Storage (eMMC 5.1 Flash)	Up to 128 GByte MLC or option for up to 64 GB pSLC
Graphics controller	Intel® UHD Gfx Gen11
SPI Boot flash	32 MByte SPI Flash chip (Winbond W25Q256JW)
Eeep	Embedded EEPROM stores modules parameters. Operates at 1.8V (I2C slave Address A0 hex 8-bit format or 50 hex 7-bit format)
Power Management	C-states: C0, C1, C6, C7, C8, C9, C10 Power Management CARIER_PWR-ON, CARRIER-STBY_ON; POWER-BTN; LID; SLEEP; RESET_OUT; RESET_IN; VIN-PWR-BAD and BATLOW
SMARC I/O System Interconnection	
Ethernet	Up to 3x 1 GbE (2x GBE0/1 and 1x optional SGMII via SERDES)
Storage	1x SATA 6Gb/s
PCI Express®	Up to 4x PCIe x1 or Option: 3x PCIe and 1x SERDES
Panel Signal	1x LVDS dual channel (on request eDP) 1x DP++ 1x HDMI (on request DP)
USB	2x USB 3.1 5Gb/s (incl. USB 2.0) 4x USB 2.0 (USB 2 port 3 as dual role client host)
Serial	3x Serial interfaces (2x RX/TX only)
Other Features	
TPM	Integrated TPM 2.0 capability of the Intel Platform Trust Technology (Intel PTT). Also known as firmware TPM (fTPM).
Watchdog timer	Watchdog timer supported by WDT_TIME_OUT
Audio	HD audio and I2S interfaces
I2C Bus	2x I2C
SMBus	HWM Nuvoton NCT7802Y (SM-Bus address: 5Ch)
SPI	2x SPI
GPIO	14x GPIO
On-Module Connectors	
Sys-Fan	Fan connector used to control fan speed operates from (3.3 V to 5.25 V input)
Power	
Power Supply	3.3 V to 5.25 V wide-range input (5 V recommended)
Software	
Operating system Support	Board Support Packages ((BSP) will be made available for: ▶ Windows® 10 ▶ Enterprise, Windows® 10 IoT ▶ Linux
BIOS	AMI Aptio V

4.5. Mechanical Specification

The SMARC short module form factor is 82 mm x 50 mm and includes four mounting holes per SMARC specification. There are two additional holes to enable the attachment of a thermal device such as a heatsink/heatspreader.

The total height of the SMARC-sXEL module depends on the height of the implemented cooling solution.

4.5.1. Mechanical Drawings

Figure 5: Dimensions of SMARC-sXEL - Industrial

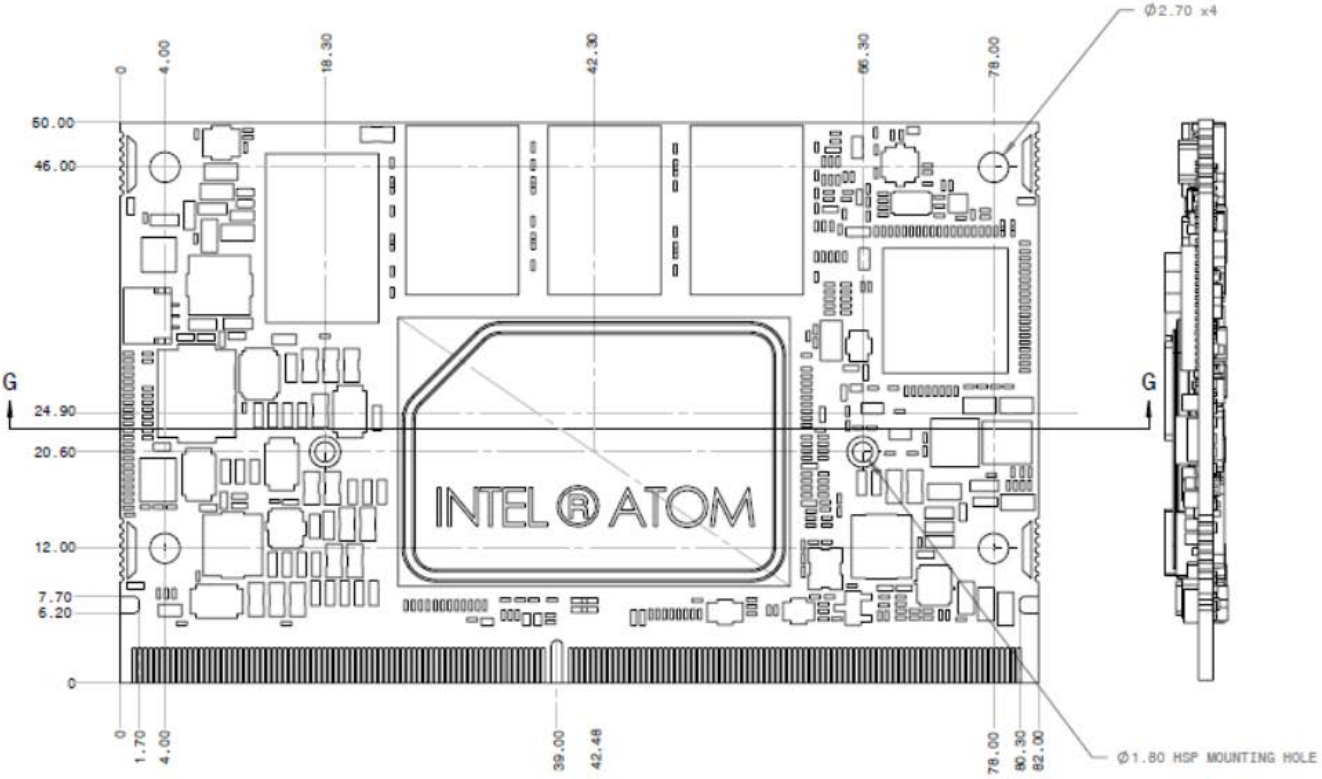


Figure 6: Thickness from the Side View - Industrial

Figure 7: Dimensions of SMARC-sXEL - Commercial

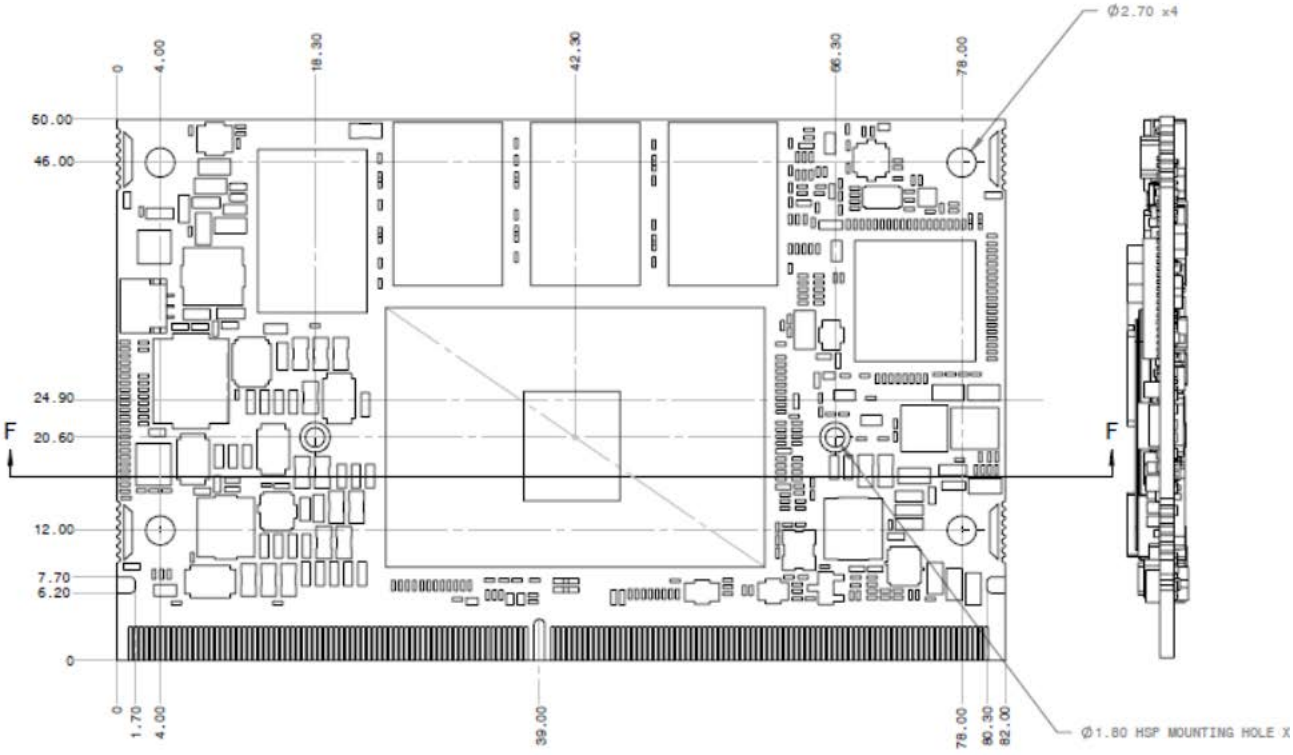
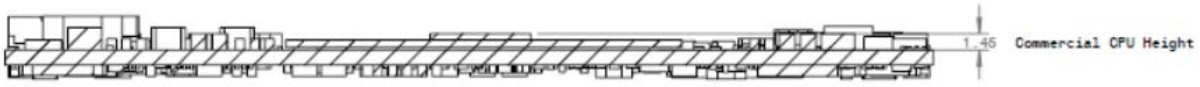


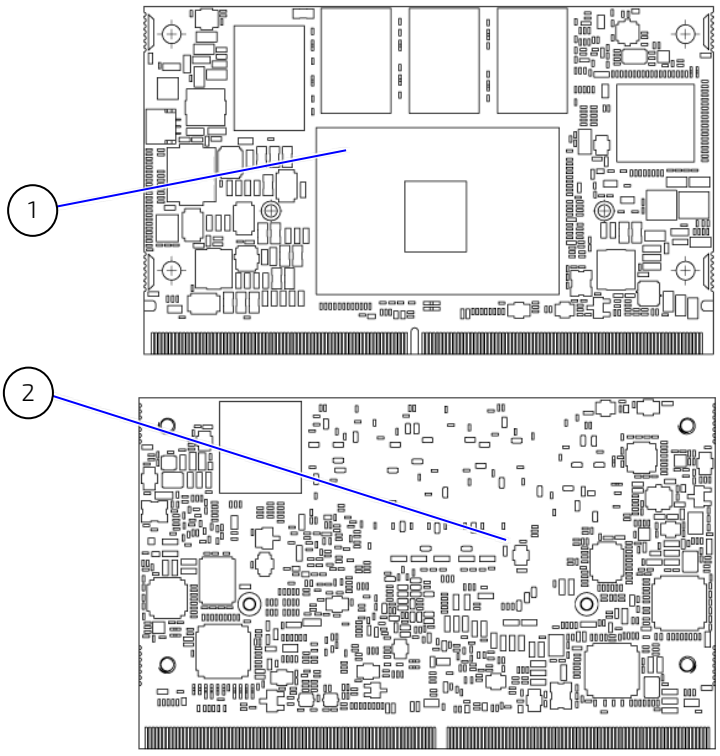
Figure 8: Thickness from the Side View, Commercial



4.6. Thermal Management Specification

The SMARC-sXEL uses an on-chip thermal sensors located within the CPU to measure the CPU temperature, and a thermal sensor close to the Hardware monitor chip to measure the module temperature.

Figure 9: Temperature Sensors



1	On-chip CPU thermal sensor	2	Hardware monitor chip temperature sensor

4.6.1. Heatspreader

A heatspreader plate assembly is available from Kontron for the SMARC-sXEL. The heatspreader plate on top of this assembly is NOT a heat sink. It works as a SMARC-standard thermal interface to use with a heat sink or external cooling devices.

External cooling must be provided to maintain the heatspreader plate at proper operating temperatures. Under worst case conditions, the cooling mechanism must maintain an ambient air and heatspreader plate temperature on any spot of the heatspreader's surface according to the module specification:

- 60°C for commercial grade modules
- 85°C for industrial temperature grade modules (E2/XT)

Documentation and CAD drawing of the heatspreader and cooling solutions are available on request from Kontron's Customer Section .

Kontron recommends the use of thermal interfaces between the heatspreader plate and the major heat-generating components. About 80 % of the power dissipated within the module is conducted to the heatspreader plate and can be removed by the cooling solution. Heatspreaders are available as an accessory for both commercial and industrial temperature grades.

Figure 10: Heatspreader as Cooling Solution

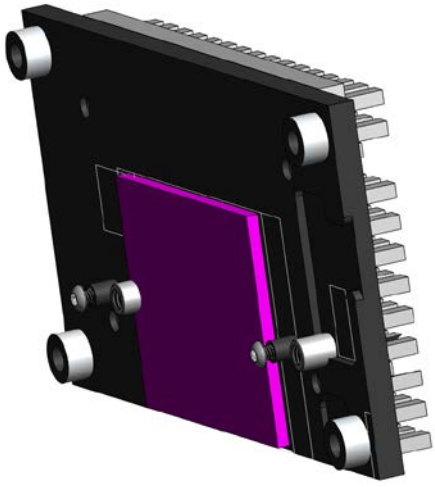


Figure 11: Heatspreader Height for Industrial Variants

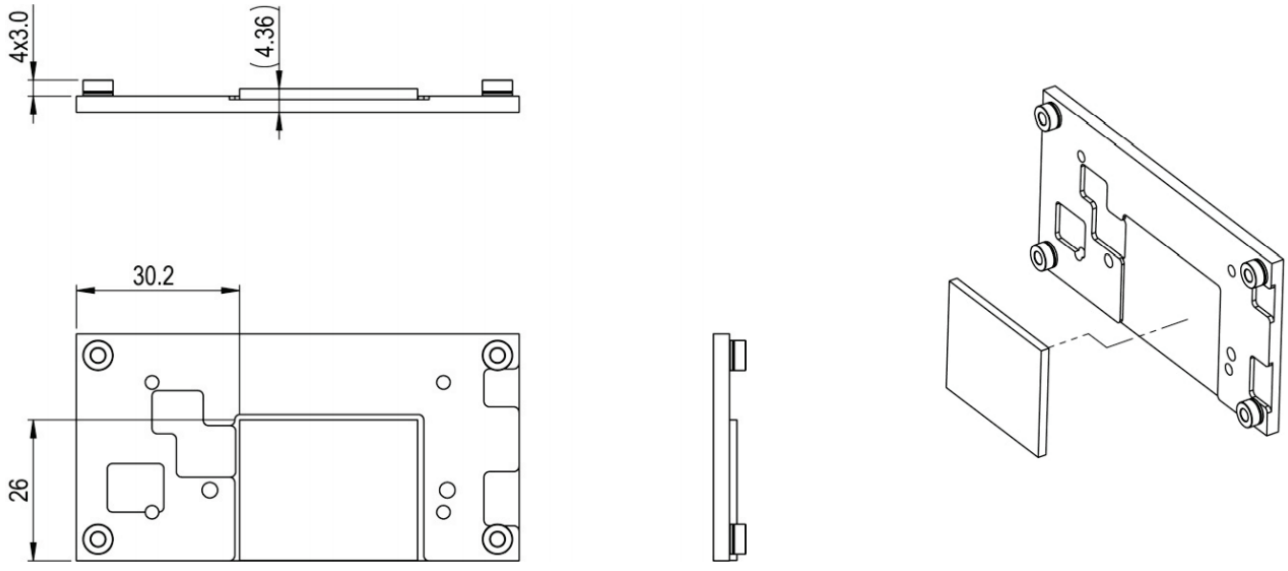
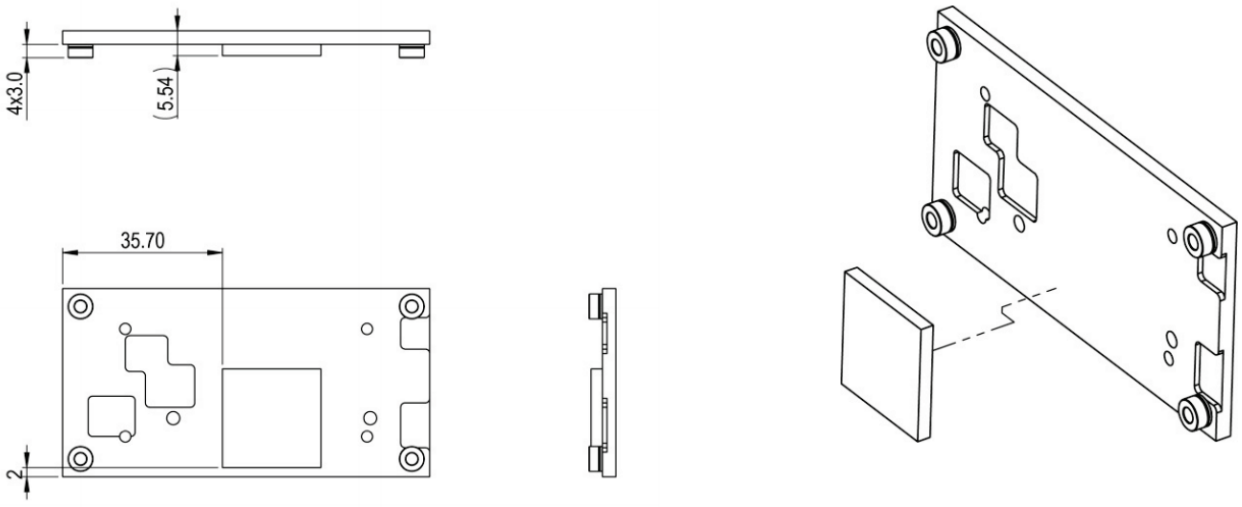


Figure 12: Heatspreader Height for Commercial Variants



4.7. Environmental Specification

Table 4: Environmental Conditions

Operating	**Temperature**	Commercial grade: 0°C to 60°C Industrial grade: -40°C to +85°C
	Humidity	93 % relative Humidity at 40 °C, non-condensing (according to IEC 60068-2-78)
Storage	**Temperature**	Commercial grade: -30°C to +85°C Industrial grade: -40°C to +85°C
	Humidity	93 % relative Humidity at 40 °C, non-condensing (according to IEC 60068-2-78)

Shock	IEC/EN 60068-2-27 Non-operating shock test (half-sinusoidal, 11 ms, 15 g)
Vibration	IEC/EN 60068-2-6 Non-operating vibration test (sinusoidal, 10 Hz – 2000 Hz, +/- 0.15 mm, 2 g)

4.8. Compliance

The SMARC-sXEL complies with the relevant requirements and the approximation of the laws relating to 'CE' and the standards that are constitutional parts of the declaration. If modified, the prerequisites for specific approvals may no longer apply. For more information, contact Kontron Support.

Table 5: Compliance CE

Europe – CE Mark	
Directives	**2014/30/EU** Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonization of the laws of the Member States relating to electromagnetic compatibility **2014/35/EU** Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonization of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits **2011/65/EU** Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment
EMC	**EN 55032:2015 /CISPR 32:2015** Electromagnetic compatibility of multimedia equipment- Emission Requirements (CISPR 32:2015); German version EN 55032:2015 **EN 61000-6-2:2005, EN 61000-6-2:2019** Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity standard for industrial environments; (IEC 61000-6-2:2005, IEC 61000-6-2:2019) German version EN/IEC 61000-6-2:2005, EN/IEC 61000-6-2:2019
Safety	**EN 62368-1:2014 + AC:2017** Audio/video, information and communication technology equipment - Part 1: Safety requirements

Table 6: Country Compliance

USA/CANADA-UL MARK	
Safety	**UL 62368-1 2nd Ed, Issued December 1, 2014** **CSA CAN/CSA-C22.2 No. 62368-1 2nd Ed, Issued December 1, 2014** Audio/video, information and communication technology equipment - Part 1: Safety requirements
International Certifications	
Safety	**IEC 62368-1:2014 2nd Ed (CB Scheme)** Audio/video, information and communication technology equipment - Part 1: Safety requirements
EMC	**IEC 61000-6-2:2005, IEC 61000-6-2:2019** Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity standard for industrial environments; (IEC 61000-6-2:2005, IEC 61000-6-2:2019) German version EN/IEC 61000-6-2:2005, EN/IEC 61000-6-2:2019

4.8.1. MTBF

Table 7: MTBF

MTBF	System MTBF (hour) = 563867 h @ 40°C for SMARC-sXEL Reliability report article number: 51017-0832-R2-4PRO

The MTBF estimated value assumes no fan, but a passive heat sinking arrangement. Estimated RTC battery life (as opposed to battery failures) is not accounted for and needs to be considered separately. Battery life depends on both temperature and operating conditions. When the module is connected to external power, the only battery drain is from leakage paths.

4.9. Power Specification

The SMARC-sXEL powers on by connecting to a carrier board via the SMARC connector. Before connecting the module to the carrier board, ensure that the carrier board is switch off and disconnected from the main power supply at the time of connection. Failure to disconnect the main power supply from the carrier board could result in personal injury and damage to the module and/or carrier board. The SMARC connector pins on the module limits the amount of power received.

The module receives power on the ten VDD-IN pins that operate over the VDD-IN range of 3.3 VDC to 5.25 VDC. The current rating of each connector pin is 0.5 A and for ten pins 5 A (0.5 A x 10).

⚠CAUTION

The SMARC-sXEL powers on by connecting to the carrier board using the Interface connector. Before connecting the module to the carrier board's corresponding connector, ensure that the carrier board is switch off and disconnected from the main power supply. Failure to disconnect the main power supply could result in personal injury and damage to the module and/or carrier board.

⚠CAUTION

Observe that only trained personnel aware of the associated dangers connect the module, within an access controlled ESD-safe workplace.

Table 8: Power Supply Voltage Requirements

Supply Voltage Range (VDD-IN)	3.3 VDC to 5.25 VDC
Supply Voltage (VDD-IN)	5 VDC (recommended)
RTC	2.0 VDC to 3.25 VDC
Input Current	5 A max. on all ten VDD_IN pins (0.5 A max. per pin)

⚠CAUTION

Only connect to an external power supply delivering the specified input rating and complying with the requirements of Safety Extra Low Voltage (SELV) and Limited Power Source (LPS) of UL/IEC 60950-1 or (PS2) of UL/IEC 62368-1.

NOTICE

To protect external power lines of peripheral devices, make sure that the wires have the right diameter to withstand the maximum available current and the enclosure of the peripheral device fulfils the fire-protection requirements of IEC/EN 62368-1.

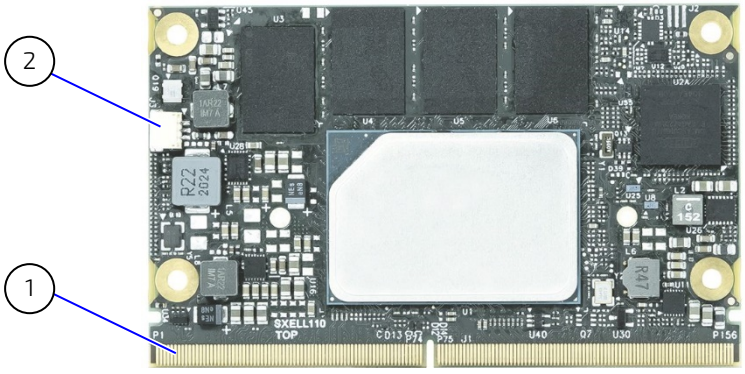
NOTICE

If an under voltage (brownout) condition occurs the used power supply must remain in the "off state" long enough to allow internal voltages to discharge sufficiently. Failure to observe this "off state" may mean that parts of the product or peripherals work incorrectly or suffer a reduction of MTBF. The minimum "off state", to allow internal voltages to discharge sufficiently, is dependent on the power supply and additional electrical factors. To determine the required "off state", each case must be considered individually. For more information, contact Kontron Support.

5/ Module and Connectors

5.1. Connectors Location

Figure 13: Connectors (top side)



3	SMARC 2.1 connector	4	3-pin fan connector

5.2. SMARC Connector

The SMARC connector is the central interface containing pins on the top and bottom sides:

- Top side: 74-pins are on the left side, 82-pins on the right side
- Bottom side: 75-pins are on the left side, 83-pins on the right side

The module's mating connector is the SMARC 2.1 (MXM3)

5.3. 3-pin Fan Connector

The 3-pin fan connector powers, controls and monitors a system fan.

Figure 14: 3-Pin Power Connector

The three pin connector is recommended for a three-wire fan to implement fan speed control. A standard 3-pin fan can be connected allowing a 5V fan to operate from a variable 3.3 VDC to 5.25 VDC power input voltage.

Table 9: Fan Connector

Connector Pin	Signal	Remark
1	FAN_TACH_CON	Input Voltage
2	V_FAN_CON	Fan Ground
3	GND	Power Ground

NOTICE Always check the fan specification according to the limitations of the supply current and supply voltage.

6/ Features and Interfaces

6.1. Processor Support

The Intel Atom®/Pentium®/Celeron® 6xxx processor family is the base for the SMARC-sXEL.

Intel® DTR (Dynamic Temperature Range)
For this processor family the Dynamic Temperature Range (DTR) behavior applies. DTR is the temperature range in which the processor can operate. The temperature range starts with the temperature of the processor (Tj = junction temperature) at boot time and can transition to a lower and/or higher temperature within the Tj min and Tj max limits.

Table 10: Supported Processors

Intel®		Celeron®	Pentium®	Celeron®	Pentium®
		J6413	J6426	N6211	N6415
# of Cores		4	4	2	4
# of Threads		4	4	2	4
Base Frequency		1.8 GHz	2.0 GHz	1.2 GHz	1.2 GHz
Turbo Frequency (Max.)		3.0 GHz	3.0 GHz	3.0 GHz	3.0 GHz
Graphic Gen 11		16 EU	32 EU	16 EU	16 EU
Thermal Design Power (TDP)		10 W	10 W	6.5 W	6.5 W
ECC Memory		No	No	No	No
Premium IO		Intel® PSE	Intel® PSE	Intel® PSE	Intel® PSE
Use Condition		PC Client	PC Client	PC Client	PC Client
Tjunction	Min.	0°C	0°C	0°C	0°C
	Max.	+105°C[2]	+105°C[2]	+105°C[2]	+105°C[2]

Intel®		Atom™	Atom®	Atom®	Atom™	Atom™	Atom™
		X6211E	X6413E	X6425E	X6212RE	X6414RE	X6425RE
# of Cores		2	4	4	2	4	4
# of Threads		2	4	4	2	4	4
Base Frequency		1.3 GHz	1.5 GHz	2.0 GHz	1.2 GHz	1.5 GHz	1.9 GHz
Turbo Frequency (Max.)		3.0 GHz	3.0 GHz	3.0 GHz			
Graphic Gen		16 EU	16 EU	32 EU	16 EU	16 EU	32 EU
Thermal Design Power (TDP)		6 W	9 W	12 W	6 W	9 W	12 W
ECC Memory		In band	In band	In band	In band	In band	In band
Premium IO		Intel® PSE	Intel® PSE	Intel® PSE	Intel®PSE/TSN Intel® TCC	Intel®PSE/TSN Intel® TCC	Intel®PSE/TSN Intel® TCC
Use Condition		Embedded	Embedded	Embedded	Industrial[1]	Industrial[1]	Industrial[1]
Tjunction	Min.	-40°C	-40°C	-40°C	-40°C	-40°C	-40°C
	Max.	+105°C[2]	+105°C[2]	+105°C[2]	+110°C[2]	+110°C[2]	+110°C[2]

[1] Recommendation for 24/7 applications.

[2] Tjunction limits for the Use Conditions:
PC Client: Tjunction limits max. temperature range during operation is +-70°C starting from boot time temperature.
Embedded: Tjunction limits the max. temperature range during operation is +-90°C starting from boot time temperature.
Industrial: Tjunction limits the max. temperature range during operation is +-110°C starting from boot time temperature.

The behavior is described in Intel document #636112 as DTR = Dynamic Temperature Range. For more information or a higher DTR-value, contact Kontron Support.

6.2. System Memory Support

The SMARC-sXEL provides two LPDDR4 banks with two devices per bank. Default LPDDR4 Memory sizes are 4 GByte (2x 16 Gb) and 8 GByte (4x 16 Gb).

The memory system has LPDDR4 memory down with in-band ECC support (1-bit correction, 2-bits detection). The module's integrated memory controller helps improve the safety and reliability by providing ECC protection to specific regions of physical memory space.

For memory capacities higher than 8 GB the maximum speed is limited to 3200 MT/s. The maximum speed of 4267 MT/s is only available for single rank chips. Dual rank chips are limited to 3733 MT/s. The module supports chip densities of 16 Gb and 32 Gb, see Table 11: LPDDR4 Memory Options.

Table 11: LPDDR4 Memory Options

	Memory Configuration	Speed
LPDDR4	1x 16 Gbit	up to 4267MT/s
	2x 16 Gbit	up to 4267MT/s
	4x 16 Gbit	up to 4267MT/s; max. 8GB
	4x 32 Gbit	up to 3200MT/s; max. 16GB

6.3. Graphics (LVDS, eDP, DP++, HDMI)

The SMARC-sXEL provides the processors Generation 11 (GEN11-LP GT1) graphics core architecture. The Gen 11 architecture supports up to 32 Execution Units (EUs) and three simultaneous displays using DDI [0-2].

The provided display technologies are DP++, HDMI 1.4 and LVDS/eDP; where the LVDS channel and control signals are pin shared with eDP signals.

Table 12: Digital Display Interfaces (DDI)

Processor Pipe	SMARC Port	
DDI0	LVDS (Single or dual channel up to 24-bits color)	eDP(option)
DDI1	DDI0 (DP++)	
DDI2	HDMI 1.4	

Due to a hardware restriction, DDI2 supports HDMI 1.4 only.

6.4. HD Audio Interfaces

The SMARC-sXEL provides two I2S audio interfaces; where one I2S Interface is pin shared with HDA. The second I2S interface can also be implemented as a HDA interface. The HDA signal level is 1.8V.

Table 13: HD Audio

SMARC Connector	PCH Pin	Description
HDA_SYNC / I2S2_LRCK	HDA_SYNC	48 kHz fixed rate sample sync to the codec(s)
HDA_SDO / I2S2_SDOUT	HDA_SDO	Serial TDM data output to the codec(s)
HDA_SDI / I2S2_SDIN	HDA_SDI0	Serial TDM data inputs from the codec(s)
HDA_CK / I2S2_CK	HDA_BCLK	24.000 MHz serial data clock generated by the Intel® HD Audio controller
GPIO4 / HDA_RST#	HDA_RST_N	Master hardware reset to external codec(s) Alternative use with GPIO4 (MUX)

Table 14: I2S Audio

SMARC Connector	PCH Pin	Description
AUDIO_MCK	AVS_I2S_MCLK1	Master Clock Output to I2S Codec(s)
I2S0_LRCK	AVS_I2S2_SFRM	I2S0 Left & Right Synchronization Clock
I2S0_SDOUT	AVS_I2S2_TXD	I2S0 Digital Audio Output
I2S0_SDIN	AVS_I2S2_RXD	I2S0 Digital Audio Input
I2S0_CK	AVS_I2S2_SCLK	I2S0 Digital Audio Clock

6.5. HSIO Overview

The SMARC-sXEL configures the high speed I/O for use as USB 3.1, PCIe 3.0, Ethernet GBE and SATA 6Gb/s as follows:

Table 15: HSIO Lane Overview

HSIO Lane#	0	1	2	3	4	5	6	7	8	9	10	11
Default	USB 0	USB 1	PCIe0	PCIe1	PCIe2	PCIe3	-	ETH0	ETH1	-	SATA0	-
Optional	USB 0	USB 1	PCIe0	PCIe1	PCIe2	-	-	ETH0	ETH1	ETH2	SATA0	-

6.6. USB

The SMARC-sXEL provides two USB 3.1 (5.0 Gb/S) SuperSpeed ports backwards compatible with USB 2.0 and four dedicated USB 2.0 ports.

Table 16: USB 3.1 Ports

SMARC Connector	ModPHY Lane	HSIO Port	Description
USB2_SS	0	USB 0	USB 3.1 (5Gb/s)
USB3_SS	1	USB 1	USB 3.1 (5Gb/s)

Table 17: USB 2.0 Ports

SMARC Connector	PCH USB Port	HSIO Port
USB0	USB2_2	-
USB1	USB2_3	-
USB2	USB2_0	-
USB3	USB2_1	Dual role Client / Host
USB4	USB2_4	-
USB5	USB2_5	-

6.6.1. USB 2.0 Client Mode

USB 2.0 port 3 provides dual role client/host. There is only one endpoint supported. Power enable /over-current detect line are shared to follow the SMARC specification.

The module does not support changing dynamically between host mode and device mode. A BIOS settings change in the BIOS setup menu and a restart is required.

6.7. PCIe 3.0

The SMARC-sXEL provides four dedicated PCIe Gen 3 lanes. The default configuration is 4 x1.

Table 18: PCIe Lanes

SMARC Connector	ModPHY Lane	HSIO Port	Supported Lane Configurations			
PCIE_A	2	PCIe 0/0	x1	x2	x2	x4
PCIE_B	3	PCIe 0/1	x1			
PCIE_C	4	PCIe 0/2	x1	x1	x2	
PCIE_D	5	PCIe 0/3	x1	x1		
	9	SGMII PSE1[1]				

[1] PCIe_D -shared with SERDES to offer 3x PCIe x1 and 1x SGMII PSE 1 for an additional LAN port.

6.8. Ethernet

The SMARC-sXEL provides two 1 Gigabit Ethernet Interfaces GBE [0-1]. Alternatively, the SMARC-sXEL supports the option of two 2.5 GbE interfaces and one additional LAN port (SGMII) via SERDES.

The two MAC Ethernet controllers GbE [0-1] are accessed via system software or the Intel® PSE and connect to the Intel® PSE (GbE PSE0 and GbE PSE1). Both MAC Ethernet controllers support Serial Gigabit Media Independent Interface (SGMII) and Reduced Gigabit Media Independent Interface (RGMII).

GbE HOST MAC is accessed through system software via PCH IO Fabric (PSF2 and PSF1) and supports the SGMII interface only.

Gigabit Ethernet Controller supports Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 2.5 G bits/sec, 1000 Mbit/sec, 100Mbit/sec and 10Mbit/sec modes.

Table 19: Ethernet Ports

SMARC connector	ModPHY Lane	HSIO Port	Description
GBE0_MDI[0-3]	7	ETH0	Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 2.5 Gb/s, 1000Mb/s, 100 Mb/s, and 10 Mb/s modes.
GBE1_MDI[1-3]	8	ETH1	Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 2.5 Gb/s, 1000 Mb/s, 100Mb/s, and 10Mb/s modes.
SERDES_0[1-3]	9	ETH3	

For 2.5 Gb/s Ethernet port speed, Intel® recommends the use of a compatible connector.

Do not use an integrated RJ45 connector module with the center tap shorted together with all 4 pairs at the center-tap transformer. This increases the common mode noise and may create EMI. Kontron recommends adding a discrete common choke in series with each PHY MDI differential line pairs If this type of integrated connector module (ICM) is chosen.

6.8.1. SGMII via SERDES (option)

The optional LAN port (SGMII) for SERDES. The SERDES pin connection is shared with PCIe_D and if implemented only three PCIe lanes are available.

6.8.2. Link and Activity LEDs

The link and activity LED signals to the carrier are configured using of PHY LED pins (GPHY_LED[0:2]) and the BIOS and GPY IC firmware.

Table 20: GBE LEDs

SMARC Connector	GbE PHY Pin	Description
GBE0_LINK_ACT#	GPHY_LED0 (U39)	Blinking – Activity on this port
GBE1_LINK_ACT#	GPHY_LED0 (U29)	
GBE0_LINK1000#	GPHY_LED2 (U39)	Amber on – Operates as a Gigabit connection (1000 Mbps)
GBE1_LINK1000#	GPHY_LED2 (U29)	
GBE0_LINK100#	GPHY_LED1 (U39)	Green on – Operates as a 100-Mbps connection
GBE1_LINK100#	GPHY_LED1 (U29)	

6.9. SATA 3.0

The SMARC-sXEL provides one SATA III 6Gb/s port.

Table 21: SATA Ports

SMARC connector	ModPHY Lane	HSIO Port	Description
SATA0	10	SATA 0	SATA 6Gb/s to SMARC gold finger

6.10. CAN Bus Interfaces

The CAN BUS communication according to ISO 11898-1 (identical to the Bosch CAN Protocol Specification 2.0 part A, B) and according to ISO 11898-4 (Time-triggered Communication on CAN).

The Can Bus controller supports communication according to CAN FD Protocol Specification 1.0. The CAN FD option can be used together with event-triggered CAN communication.

Table 22: CAN Bus

SMARC Connector	EHL Pin	Description
CAN0_TX	PSE_CAN0_TX	Can Port 0 transmit output
CAN0_RX	PSE_CAN0_RX	Can Port 0 Receive output
CAN1_TX	PSE_CAN1_TX	Can Port 1 transmit output
CAN1_RX	PSE_CAN1_RX	Can Port 1 receive output

6.11. Eeep

The embedded EEPROM (EeeP) is connected to I2C_GP bus from the CPLD and operates at 1.8 V. The EeeP address is A0h (8bit format). The EEPROM retains module parameter information, including the module serial number and data structure and conforms to the PICMG® EEEP Embedded EEPROM Specification.

6.12. eMMC Flash Memory (option)

The Embedded Multimedia Flash Card (eMMC) is eMMC 5.1 compatible. The standard eMMC Flash memory is MLC. On request eMMC pSLC can be offered. During the manufacturing process, Multi Level Cell (MLC) eMMC is reconfigured to act as pseudo Single Level Cell (pSLC) eMMC to provide improved reliability, endurance and performance.

The module's eMMC flash memory supports up to 64 GByte pSLC or 128 GByte MLC.

Table 23: eMMC Flash Memory

eMMC NAND Flash	Product Name
64 GByte	MTFC64GAPALBH-IT
32 GByte	MTFC32GAPALBH-IT
16 GByte	MTFC16GAPALBH-IT

6.13. I2C Bus Support

The SMARC-sXEL contains two I2C interfaces I2C_GP and I2C_INT capable and data rates of 100 kHz and 400 kHz.

6.14. Kontron CPLD

The embedded controlled implements Kontron CPLD Specification, KCPLD is connect to EHL eSPI interface to provide the following module/carrier features:

- I2C
- UART
- GPIO
- Watchdog

The embedded controller is responsible for the power sequence and reset control for all components.

Table 24: Kontron CPLD

PCH PIN	CPLD I/O	Description
GP_G[15:18] / ESPI_IO[0:3]	G10, F12, F13, E13	
GP_G21 / ESPI_CLK	G9	Dedicated clock pin
GP_G22 / ESPI_RST0_N	F9	
GP_G20 / ESPI_CS0_N	F10	
GP_B03 / ESPI_ALERT0_N	E12	

6.15. RTC

The RTC keeps track of the current time accurately. The RTC's low power consumption means that the RTC can be powered from an alternative source of power enabling the RTC to continue to keep time while the primary source of power is off or unavailable.

The RTC's battery voltage range is 2.0 V to 3.25 V. Typical RTC values are 3 V and less than 10 µA. If the module is powered by mains supply, the RTC voltage is generated by on-module regulators, to reduce RTC current draw.

The SMARC-sXEL supports an internal RTC by default with the option for an external RTC on request such as a lithium cell or super cap on the carrier board.

Using the SMARC-sXEL without RTC battery voltage supply may result in improper behavior. Contact Kontron Support in case you plan a carrier design without RTC battery.

6.16. SDIO

The SDIO interface supports a 4-bit SD card with support lines on the carrier board. The SD Cards voltage level is 3.3V.

Table 25: SDIO Interface

SMARC Connector	EHL Pin	Description
SDIO_WP	SD_SDIO_WP	SDIO Write Protect Denotes the state of the write-protect tab on SD cards.
SDIO_CMD	SDCARD_CMD	SDIO Command/Response For card initialization and for command transfers. During initialization mode this signal is open drain. During command transfer this signal is in push-pull mode.
SDIO_CD#	SD_SDIO_CD_N	SDIO Card Detect Indicates when a SDIO/MMC card is present.
SDIO_CK	SD_SDIO_CLK	SDIO Clock With each cycle a one-bit transfer on the command and each data line occurs.
SDIO_PWR_EN	SD_SDIO_PWR_EN_N	SDIO Power Enable Enable the power being supplied to a SD/MMC card device.
SDIO_D[3:0]	SD_SDIO_D[3:0]	SDIO Data lines These signals operate in push-pull mode at 3.3 V

6.17. SPI Interfaces

The Serial Peripheral Interface (SPI) bus is a synchronous serial data link where devices communicate in master/slave mode and the master device initiates the data frame. Multiple slave devices are allowed with individual slave select (chip select) lines.

The SPI interface may only be used with a SPI Flash device to boot from the external BIOS on the carrier board.

The SMARC-sXEL supports two SPI interfaces.

- SMARC connector SPI0 connects to the EHL FSPI. This interfaces supports serial flash for BIOS firmware. FSPI supports on-module and carrier boot from SPI according to boot select setting.
- SMARC connector's SPI1 connects to the EHL general purpose SIO_SPI2.

General purpose SPI is provided by the SMARC Eval Carrier eSPI connector (J47).

6.17.1. SPI Boot Flash Chip

The SPI Flash chip stores the BIOS to be booted. The SMARC-sXEL supports SPI boot from the 32 MByte SPI Flash chip on the board and an external 32 MByte SPI Flash chip on the carrier board.

The SPI flash chip on the carrier is required to be 32MByte (256MBit).

The module's SPI voltage is 1.8V. Booting takes place either from the on-module SPI Flash chip or the external SPI Flash chip on the carrier board. To select the SPI to boot from, see Chapter 8.1: Boot Select.

The supported SPI Boot Flash Types for are listed in the following table.

Table 26: Supported SPI Boot Flash Types

Size	Manufacturer	Part Number	Device ID
32MB	Winbond	W25Q256JW	EFh / 60h / 19h

6.18. TPM 2.0

The Trusted Platform Module (TPM) 2.0 technology stores RSA encryption keys specific to the host system for hardware authentication

Each TPM contains an RSA key pair called the Endorsement Key (EK). The pair is maintained inside the TPM and cannot be accessed by software. The Storage Root Key (SRK) is created when a user or administrator takes ownership of the system. This key pair is generated by the TPM based on the Endorsement Key and an owner-specified password.

A second key, called an Attestation Identity Key (AIK) protects the device against unauthorized firmware and software modification by hashing critical sections of firmware and software before they are executed. When the system attempts to connect to the network, the hashes are sent to a server that verifies they match the expected values. If

any of the hashed components have been modified since the last start, the match fails, and the system cannot gain entry to the network.

The SMARC-sXEL supports the built-in CPU firmware TPM (fTPM) using the integrated TPM 2.0 capability of the Intel Platform Trusted Technology (Intel® PTT). Also known as firmware TPM (fTPM). Hardware TPM is an option.

6.19. UART Interfaces

The UART serial communications interface option supports up to three serial RX/TX ports defined, where one port is supported by the PCH and two ports are supported by the on-module CPLD.

The UART option is 16550 compatible and features:

- 64-byte TX /RX host controller FIFOs
- On-chip bit rate (baud rate) generator
- Prioritized interrupt identification
- Programmable FIFO enable/disable

Table 27: UART Serial Port

SMARC Connector	PCH Pin	CPLD Pin	Description
SER0_TX	SIO_UART1_TXD		Asynchronous Serial Data Output Port 0
SER0_RX	SIO_UART1_RXD		Asynchronous Serial Data Input Port 0
SER0_RTS#	SIO_UART1_RTS_N		Request to Send Handshake Line for Port 0
SER0_CTS#	SIO_UART1_CTS_N		Clear to Send Handshake Line for Port 0
SER1_TX		po_uart_tx[0]	
SER1_RX		po_uart_rx[0]	
SER3_TX		po_uart_tx[1]	
SER3_RX		po_uart_rx[1]	

7/ Pin Definitions

The following sections provide pin definitions and detailed description of all on-board connectors. The connector definitions follow the following notation.

Table 28: Connector Definitions

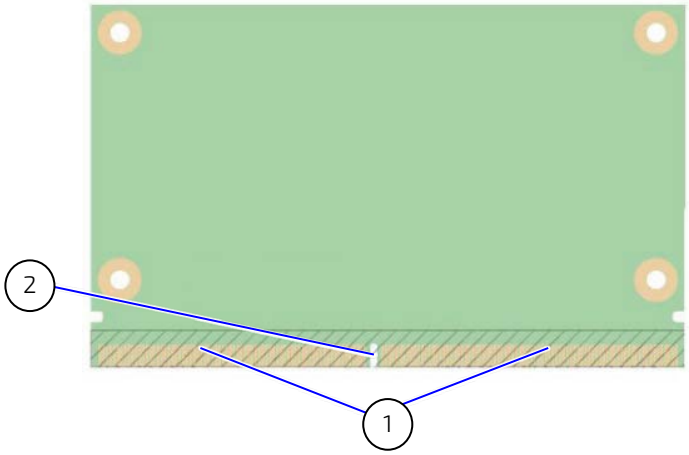
Product Number	Description
Pin	**S**hows the pin-numbers in the connector. The graphical layout of the connector definition tables is made similar to the physical connectors.
Signal	The mnemonic name of the signal at the current pin. The notation "XX#" states that the signal "XX" is active low.
Type	**AI**: AI: Analog Input AO: AO: Analog Output I I: Input, TTL compatible if nothing else stated IO IO: Input / Output, TTL compatible if nothing else stated IOT: IOT: Bi-directional tristate IO pin. IS:. IS: Schmitt-trigger input, TTL compatible. IOC IOC: Input / open-collector Output, TTL compatible IOD IOD: Input / Output, CMOS level Schmitt-triggered (Open drain output) NC NC: Not Connected O: Output, TTL compatible OC OC: Output, open-collector or open-drain, TTL compatible OT OT: Output with tri-state capability, TTL compatible LVDS LVDS: Low Voltage Differential Signal PWR PWR: Power supply or ground reference pins
	Ioh: Typical current in mA flowing out of an output pin through a grounded load, while the output voltage is > 2.4 V DC (if nothing else stated). Iol: Typical current in mA flowing into an output pin from a VCC connected load, while the output voltage is < 0.4 V DC (if nothing else stated)
Pull U/D	On-board pull-up or pull-down resistors on input pins or open-collector output pins
Note	Special remarks concerning the signal
Designation	**T**ype and number of item described

7.1. Smart Connector

The SMARC connector has different pins on both sides:

- Top side: 74-pins are on the left side, 82-pins on the right side
- Bottom side: 75-pins are on the left side, 83-pins on the right side

Figure 15: SMARC Connector 314-Pin



1 Top side connector pins P[1-156] and on the reverse side, bottom side connector pins S[1-158]

2 Connector-key gap

Table 29: SMARC Pinout Legend

Signal	Description
DP-I	Differential Pair Input
DP-I/O	Differential Pair Input/Output
I/O-3.3	Bi-directional 3.3 V I/O signal
I-3.3	3.3 V Input
PWRGND	Power Ground
OD	Output Open Drain
NC	Not Connected
o-1.8	1.8 V Output
DP-O	Differential Pair Output
I/O-1.8	Bi-directional 1.8 V I/O signal
I-5.0	5.0 V Input
0-3.3	3.3 V Output

7.1.1. Pinout of SMARC Connector (Top Side)

Table 30: SMARC 2.1 Specification Pinout (Top side)

P-PIN	Primary	Description	Type	Termin-ation	Comment
P1	SMB_ALERT#	SMBus Alert# (Interrupt) Signal	I OD CMOS 1.8 to 5 V	PU 2k2	
P2	GND				
P3	CSI1_CK+	CSI1 differential clock input (point to point)	I D-PHY		Not Connected
P4	CSI1_CK-	CSI1 differential clock input (point to point)	I D-PHY		Not Connected

<table>
<tr><th>P-PIN</th><th>Primary</th><th>Description</th><th>Type</th><th>Termin-ation</th><th>Comment</th></tr>
<tr><td>P5</td><td>GBE1_SDP</td><td>IEEE 1588 Trigger Signal for Hardware Implementation of PTP (Precision Time Protocol)</td><td>I/O CMOS 3.3V</td><td></td><td></td></tr>
<tr><td>P6</td><td>GBE0_SDP</td><td>IEEE 1588 Trigger Signal for Hardware Implementation of PTP (Precision Time Protocol)</td><td>I/O CMOS 3.3V</td><td></td><td></td></tr>
<tr><td>P7</td><td>CSI1_RX0+</td><td>CSI1 differential input (point to point)</td><td>I D-PHY / I M-PHY</td><td></td><td>Not Connected</td></tr>
<tr><td>P8</td><td>CSI1_RX0-</td><td>CSI1 differential input (point to point)</td><td>I D-PHY / I M-PHY</td><td></td><td>Not Connected</td></tr>
<tr><td>P9</td><td>GND</td><td></td><td></td><td></td><td></td></tr>
<tr><td>P10</td><td>CSI1_RX1+</td><td>CSI1 differential input (point to point)</td><td>I D-PHY / I M-PHY</td><td></td><td>Not Connected</td></tr>
<tr><td>P11</td><td>CSI1_RX1-</td><td>CSI1 differential input (point to point)</td><td>I D-PHY / I M-PHY</td><td></td><td>Not Connected</td></tr>
<tr><td>P12</td><td>GND</td><td></td><td></td><td></td><td></td></tr>
<tr><td>P13</td><td>CSI1_RX2+</td><td>CSI1 differential input (point to point)</td><td>I D-PHY / I M-PHY</td><td></td><td>Not Connected</td></tr>
<tr><td>P14</td><td>CSI1_RX2-</td><td>CSI1 differential input (point to point)</td><td>I D-PHY / I M-PHY</td><td></td><td>Not Connected</td></tr>
<tr><td>P15</td><td>GND</td><td></td><td></td><td></td><td></td></tr>
<tr><td>P16</td><td>CSI1_RX3+</td><td>CSI1 differential input (point to point)</td><td>I D-PHY / I M-PHY</td><td></td><td>Not Connected</td></tr>
<tr><td>P17</td><td>CSI1_RX3-</td><td>CSI1 differential input (point to point)</td><td>I D-PHY / I M-PHY</td><td></td><td>Not Connected</td></tr>
<tr><td>P18</td><td>GND</td><td></td><td></td><td></td><td></td></tr>
<tr><td>P19</td><td>GBE0_MDI3-</td><td>Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations</td><td>I/O GBE MDI</td><td></td><td>Gigabit Ethernet Controller 0:
Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.
Some pairs are unused in some modes according to the following:
<table>
<tr><th></th><th>1000</th><th>100</th><th>10</th></tr>
<tr><td>MDI0 +/-</td><td>B1_DA+/-</td><td>TX+/-</td><td>TX+/-</td></tr>
<tr><td>MDI1 +/-</td><td>B1_DB+/-</td><td>RX+/-</td><td>RX+/-</td></tr>
<tr><td>MDI2 +/-</td><td>B1_DC+/-</td><td></td><td></td></tr>
<tr><td>MDI3 +/-</td><td>B1_DD+/-</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>P20</td><td>GBE0_MDI3+</td><td>Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations</td><td>I/O GBE MDI</td><td></td><td>Gigabit Ethernet Controller 0:
Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.
Some pairs are unused in some modes according to the following:
<table>
<tr><th></th><th>1000</th><th>100</th><th>10</th></tr>
<tr><td>MDI0 +/-</td><td>B1_DA+/-</td><td>TX+/-</td><td>TX+/-</td></tr>
<tr><td>MDI1 +/-</td><td>B1_DB+/-</td><td>RX+/-</td><td>RX+/-</td></tr>
</table></td></tr>
</table>

P-PIN	Primary	Description	Type	Termination	Comment
					MDI2 +/- | B1_DC+/- | | MDI3 +/- | B1_DD+/- | |
P21	GBE0_LINK100#	Link Speed Indication LED for GBE0 100Mbps	O OD CMOS 3.3V		Shall be able to sink 24mA or more Carrier LED current.
P22	GBE0_LINK1000#	Link Speed Indication LED for GBE0 1000Mbps	O OD CMOS 3.3V		Shall be able to sink 24mA or more Carrier LED current.
P23	GBE0_MDI2-	Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations	I/O GBE MDI		Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes. Some pairs are unused in some modes according to the following:

	1000	100	10
MDI0 +/-	B1_DA+/-	TX+/-	TX+/-
MDI1 +/-	B1_DB+/-	RX+/-	RX+/-
MDI2 +/-	B1_DC+/-		
MDI3 +/-	B1_DD+/-		

P24	GBE0_MDI2+	Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations	I/O GBE MDI		Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes. Some pairs are unused in some modes according to the following:

	1000	100	10
MDI0 +/-	B1_DA+/-	TX+/-	TX+/-
MDI1 +/-	B1_DB+/-	RX+/-	RX+/-
MDI2 +/-	B1_DC+/-		
MDI3 +/-	B1_DD+/-		

P25	GBE0_LINK_ACT#	Link / Activity Indication LED Driven Low on Link (10, 100 or 1000 Mbps) Blinks on Activity	O OD CMOS 3.3V		Shall be able to sink 24mA or more Carrier LED current.
P26	GBE0_MDI1-	Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations	I/O GBE MDI		Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes. Some pairs are unused in some modes according to the following:

	1000	100	10
MDI0 +/-	B1_DA+/-	TX+/-	TX+/-
MDI1 +/-	B1_DB+/-	RX+/-	RX+/-

<table>
<tr><th>P-PIN</th><th>Primary</th><th>Description</th><th>Type</th><th>Termin-ation</th><th>Comment</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>
<table>
<tr><td>MDI2 +/-</td><td>B1_D C+/-</td><td></td><td></td></tr>
<tr><td>MDI3 +/-</td><td>B1_D D+/-</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>P27</td><td>GBE0_MDI1+</td><td>Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations</td><td>I/O GBE MDI</td><td></td><td>Gigabit Ethernet Controller 0:
Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.
Some pairs are unused in some modes according to the following:
<table>
<tr><td></td><td>1000</td><td>100</td><td>10</td></tr>
<tr><td>MDI0 +/-</td><td>B1_D A+/-</td><td>TX+/ -</td><td>TX+/ -</td></tr>
<tr><td>MDI1 +/-</td><td>B1_D B+/-</td><td>RX+/ -</td><td>RX+/ -</td></tr>
<tr><td>MDI2 +/-</td><td>B1_D C+/-</td><td></td><td></td></tr>
<tr><td>MDI3 +/-</td><td>B1_D D+/-</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>P28</td><td>GBE0_CTREF</td><td>Center-Tap Reference Voltage for Carrier Board Ethernet Magnetic (if required by the Module GBE PHY)</td><td>Analog 0 to 3.3V max</td><td></td><td></td></tr>
<tr><td>P29</td><td>GBE0_MDI0-</td><td>Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations</td><td>I/O GBE MDI</td><td></td><td>Gigabit Ethernet Controller 0:
Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.
Some pairs are unused in some modes according to the following:
<table>
<tr><td></td><td>1000</td><td>100</td><td>10</td></tr>
<tr><td>MDI0 +/-</td><td>B1_D A+/-</td><td>TX+/ -</td><td>TX+/ -</td></tr>
<tr><td>MDI1 +/-</td><td>B1_D B+/-</td><td>RX+/ -</td><td>RX+/ -</td></tr>
<tr><td>MDI2 +/-</td><td>B1_D C+/-</td><td></td><td></td></tr>
<tr><td>MDI3 +/-</td><td>B1_D D+/-</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>P30</td><td>GBE0_MDI0+</td><td>Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations</td><td>I/O GBE MDI</td><td></td><td>Gigabit Ethernet Controller 0:
Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.
Some pairs are unused in some modes according to the following:
<table>
<tr><td></td><td>1000</td><td>100</td><td>10</td></tr>
<tr><td>MDI0 +/-</td><td>B1_D A+/-</td><td>TX+/ -</td><td>TX+/ -</td></tr>
<tr><td>MDI1 +/-</td><td>B1_D B+/-</td><td>RX+/ -</td><td>RX+/ -</td></tr>
<tr><td>MDI2 +/-</td><td>B1_D C+/-</td><td></td><td></td></tr>
</table>
</td></tr>
</table>

P-PIN	Primary	Description	Type	Termination	Comment
					MDI3 +/- | B1_D D+/- |	
P31	SPI0_CS1#	SPI0 Master Chip Select 1	O CMOS 1.8V		
P32	GND				
P33	SDIO_WP	SDIO Write Protect. This signal denotes the state of the write-protect tab on SD cards.	I OD CMOS 1.8V / 3.3V	PU 10k	
P34	SDIO_CMD	SDIO Command/Response. This signal is used for card initialization and for command transfers. During initialization mode this signal is open drain. During command transfer this signal is in push-pull mode.	I/O CMOS 1.8V / 3.3V		SDIO controller may detect SD Cards voltage level (1.8V for UHS-I and 3.3V for standard) and adjust its I/O voltage level accordingly
P35	SDIO_CD#	SDIO Card Detect. This signal indicates when a SDIO/MMC card is present.	I OD CMOS 1.8V / 3.3V	PU 10k	
P36	SDIO_CK	SDIO Clock. With each cycle of this signal a one-bit transfer on the command and each data line occurs.	O CMOS 1.8V / 3.3V		SDIO controller will detect SD Cards voltage level (1.8V for UHS-I and 3.3V for standard) and adjust its I/O voltage level accordingly
P37	SDIO_PWR_EN	SDIO Power Enable. This signal is used to enable the power being supplied to a SD/MMC card device.	O CMOS 3.3V		Should be driven low in Standby Mode by the Module
P38	GND				
P39	SDIO_D0	SDIO Data lines. These signals operate in push-pull mode.	I/O CMOS 1.8V / 3.3V		SDIO controller may detect SD Cards voltage level (1.8V for UHS-I and 3.3V for standard) and adjust its I/O voltage level accordingly
P40	SDIO_D1	SDIO Data lines. These signals operate in push-pull mode.	I/O CMOS 1.8V / 3.3V		SDIO controller may detect SD Cards voltage level (1.8V for UHS-I and 3.3V for standard) and adjust its I/O voltage level accordingly
P41	SDIO_D2	SDIO Data lines. These signals operate in push-pull mode.	I/O CMOS 1.8V / 3.3V		SDIO controller may detect SD Cards voltage level (1.8V for UHS-I and 3.3V for standard) and adjust its I/O voltage level accordingly
P42	SDIO_D3	SDIO Data lines. These signals operate in push-pull mode.	I/O CMOS 1.8V / 3.3V		SDIO controller may detect SD Cards voltage level (1.8V for UHS-I and 3.3V for standard) and adjust its I/O voltage level accordingly
P43	SPI0_CS0#	SPI0 Master Chip Select 0	O CMOS 1.8V		This signal can be used to select Carrier SPI as boot device
P44	SPI0_CK	SPI0 Clock	O CMOS 1.8V		
P45	SPI0_DIN	SPI0 Master input / Slave output	I CMOS 1.8V		also referred to as MISO
P46	SPI0_DO	SPI0 Master output / Slave input	O CMOS 1.8V		also referred to as MOSI
P47	GND				
P48	SATA_TX+	Serial ATA Channel 0 Transmit Output Differential Pair	O SATA		Series AC coupled on Module 10nF

P-PIN	Primary	Description	Type	Termination	Comment
P49	SATA_TX-	Serial ATA Channel 0 Transmit Output Differential Pair	O SATA		Series AC coupled on Module 10nF
P50	GND				
P51	SATA_RX+	Serial ATA Channel 0 Receive Input Differential Pair	I SATA		Series AC coupled on Module 10nF
P52	SATA_RX-	Serial ATA Channel 0 Receive Input Differential Pair	I SATA		Series AC coupled on Module 10nF
P53	GND				
P54	ESPI_CS0# / SPI1_CS0# / QSPI_CS0#	ESPI1 Master Chip Select 0	O CMOS 1.8V		
		SPI1 Master Chip Select 0	O CMOS 1.8V		
		QSPI Master Chip Select 0	O CMOS 1.8V		
P55	ESPI_CS1# / SPI1_CS1# / QSPI_CS1#	ESPI1 Master Chip Select 1	O CMOS 1.8V		
		SPI1 Master Chip Select 1	O CMOS 1.8V		
		QSPI Master Chip Select 1	O CMOS 1.8V		
P56	ESPI_CK / SPI1_CK / QSPI_CK	ESPI Master Clock Output	O CMOS 1.8V		
		SPI1 Clock	O CMOS 1.8V		
		QSPI Clock	O CMOS 1.8V		
P57	ESPI_IO_1 / SPI1_DIN / QSPI_IO_1	ESPI Master Data Input / Output	I/O CMOS 1.8V		In Single I/O mode, ESPI_IO_0 is the eSPI master output / eSPI slave input (MOSI) whereas ESPI_IO_1 is the SPI master input / eSPI slave output (MISO).
		SPI1 Master input / Slave output	I CMOS 1.8V		also referred to as MISO
		QSPI Data input / output	I/O CMOS 1.8V		
P58	ESPI_IO_0 / SPI1_DO / QSPI_IO_0	ESPI Master Data Input / Output	I/O CMOS 1.8V		In Single I/O mode, ESPI_IO_0 is the eSPI master output / eSPI slave input (MOSI) whereas ESPI_IO_1 is the SPI master input / eSPI slave output (MISO).
		SPI1 Master output / Slave input	O CMOS 1.8V		also referred to as MOSI
		QSPI Data input / output	I/O CMOS 1.8V		
P59	GND				
P60	USB0+	USB Differential Data Pairs for Port 0	I/O USB		
P61	USB0-	USB Differential Data Pairs for Port 0	I/O USB		
P62	USB0_EN_OC#	USB Over-Current Sense for Port 0	I/O OD CMOS 3.3V	PU 10k	Pulled low by Module OD driver to disable USB0 power. Pulled low by Carrier OD driver to indicate over-current situation.
P63	USB0_VBUS_DET	USB Port 0 Host Power Detection	I USB VBUS 5V		When this Port is used as a device it can be connected to a USB client port VBUS pin.
P64	USB0_OTG_ID	Input Pin to Announce OTG Device Insertion on USB 2.0 Port			Resistor value to ground according to USB specification
P65	USB1+	USB Differential Data Pairs for Port 1	I/O USB		

P-PIN	Primary	Description	Type	Termination	Comment
P66	USB1-	USB Differential Data Pairs for Port 1	I/O USB		
P67	USB1_EN_OC#	USB Over-Current Sense for Port 1	I/O OD CMOS 3.3V	PU 10k	Pulled low by Module OD driver to disable USB1 power. Pulled low by Carrier OD driver to indicate over-current situation.
P68	GND				
P69	USB2+	USB Differential Data Pairs for Port 2	I/O USB		
P70	USB2-	USB Differential Data Pairs for Port 2	I/O USB		
P71	USB2_EN_OC#	USB Over-Current Sense for Port 2	I/O OD CMOS 3.3V	PU 10k	Pulled low by Module OD driver to disable USB2 power. Pulled low by Carrier OD driver to indicate over-current situation.
P72	RSVD				
P73	RSVD				
P74	USB3_EN_OC#	USB Over-Current Sense for Port 3	I/O OD CMOS 3.3V	PU 10k	Pulled low by Module OD driver to disable USB3 power. Pulled low by Carrier OD driver to indicate over-current situation
P75	PCIE_A_RST#	PCIe Port A reset output	O CMOS 3.3V		
P76	USB4_EN_OC#	USB Over-Current Sense for Port 4	I/O OD CMOS 3.3V	PU 10k	Pulled low by Module OD driver to disable USB4 power. Pulled low by Carrier OD driver to indicate over-current situation.
P77	PCIE_B_CKREQ#	PCIe Port B clock request	IO OD CMOS 3.3V	>10k PU	Can be used for power saving mode on PCIe - Pulled up or terminated on Module
P78	PCIE_A_CKREQ#	PCIe Port A clock request	IO OD CMOS 3.3V	>10k PU	Can be used for power saving mode on PCIe - Pulled up or terminated on Module
P79	GND				
P80	PCIE_C_REFCK+	Differential PCIe Link C reference clock output	O PCIE		
P81	PCIE_C_REFCK-	Differential PCIe Link C reference clock output	O PCIE		
P82	GND				
P83	PCIE_A_REFCK+	Differential PCIe Link A reference clock output	O PCIE		
P84	PCIE_A_REFCK-	Differential PCIe Link A reference clock output	O PCIE		
P85	GND				
P86	PCIE_A_RX+	Differential PCIe link A receive data pair	I PCIE		Series AC coupled off Module 75-265nF depending on PCIe generation
P87	PCIE_A_RX-	Differential PCIe link A receive data pair	I PCIE		Series AC coupled off Module 75-265nF depending on PCIe generation
P88	GND				
P89	PCIE_A_TX+	Differential PCIe link A transmit data pair	O PCIE		Series AC coupled on Module 75-265nF depending on PCIe generation
P90	PCIE_A_TX-	Differential PCIe link A transmit data pair	O PCIE		Series AC coupled on Module 75-265nF depending on PCIe generation
P91	GND				

P-PIN	Primary	Description	Type	Termination	Comment
P92	HDMI_D2+ / DP1_LANE0+	HDMI Port, Differential Pair Data Lines	O TMDS HDMI		
		Secondary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
P93	HDMI_D2- / DP1_LANE0-	HDMI Port, Differential Pair Data Lines	O TMDS HDMI		
		Secondary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
P94	GND				
P95	HDMI_D1+ / DP1_LANE1+	HDMI Port, Differential Pair Data Lines	O TMDS HDMI		
		Secondary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
P96	HDMI_D1- / DP1_LANE1-	HDMI Port, Differential Pair Data Lines	O TMDS HDMI		
		Secondary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
P97	GND				
P98	HDMI_D0+ / DP1_LANE2+	HDMI Port, Differential Pair Data Lines	O TMDS HDMI		
		Secondary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
P99	HDMI_D0- / DP1_LANE2-	HDMI Port, Differential Pair Data Lines	O TMDS HDMI		
		Secondary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
P100	GND				
P101	HDMI_CK+ / DP1_LANE3+	HDMI Port, Differential Pair Data Lines	O TMDS HDMI		
		Secondary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
P102	HDMI_CK- / DP1_LANE3-	HDMI Port, Differential Pair Data Lines	O TMDS HDMI		
		Secondary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
P103	GND				
P104	HDMI_HPD / DP1_HPD	HDMI Hot Plug Active High Detection Signal that Serves as an Interrupt Request	I CMOS 1.8V	PD 1M	Important: Module shall tolerate high level in stand-by mode
		DP Hot Plug Detect Input	I CMOS 1.8V	PD 1M	Module must tolerate high level in stand-by mode. The Carrier shall include a blocking FET on DP1_HPD to prevent back-drive current from damaging the Module.
P105	HDMI_CTRL_CK / DP1_AUX+	I2C_CLK Line Dedicated to HDMI	I/O OD CMOS 1.8V	PU 100K	Level shifter FET and 5V PU resistor shall be placed between the Module and the HDMI connector. Stronger pull-up is demanded to the carrier board. The pull-ups may be part of an integrated HDMI ESD protection and control-line level shift device, such as the Texas Instruments TPD12S016. If discrete Carrier pull-ups are used, the value

P-PIN	Primary	Description	Type	Termination	Comment
					depends on the individual carrier board implementation.
		Secondary DP Port. Bidirectional Channel used for Link Management and Device Control	I/O DP 3.3V	PD 100k	AC coupled on Module. If DP1_AUX_SEL=0 (DP mode): AC coupled on module, 100k PD. If DP1_AUX_SEL=1 (HDMI mode): DC coupled, CMOS, 100k PU. In case of HDMI over DP++ implementation, stronger pull-up is demanded to the Carrier Board.
P106	HDMI_CTRL_DAT / DP1_AUX-	I2C_DAT Line Dedicated to HDMI	I/O OD CMOS 1.8V	PU 100K	Level shifter FET and 5V PU resistor shall be placed between the Module and the HDMI connector. Stronger pull-up is demanded to the carrier board. The pull-ups may be part of an integrated HDMI ESD protection and control-line level shift device, such as the Texas Instruments TPD12S016. If discrete Carrier pull-ups are used, the value depends on the individual carrier board implementation.
		Secondary DP Port Bidirectional Channel used for Link Management and Device Control	I/O DP 3.3V	PU 100k	AC coupled on Module. If DP1_AUX_SEL=0 (DP mode): AC coupled on module, 100k PU. If DP1_AUX_SEL=1 (HDMI mode): DC coupled, CMOS, 100k PU. In case of HDMI over DP++ implementation, stronger pull-up is demanded to the Carrier Board.
P107	DP1_AUX_SEL	Strapping Signal to Enable Either HDMI or DP Output	I CMOS 1.8V	PD 1M	Pulled to GND on Carrier for DP operation in Dual Mode (DP++) implementations. Driven to 1.8V on Carrier for HDMI mode. Module must tolerate high level in stand-by mode. Should be connected to pin 13 of the DisplayPort connector to enable a dual-mode DisplayPort interface.
P108	GPIO0 / CAM0_PWR#	Camera 0 Power Enable, active low output.	O CMOS 1.8V		Shared with GPIO0
		GPIO Pin 0 Preferred Output	I/O CMOS 1.8V	PU 470k	Alternative use: CAM0_PWR#
P109	GPIO1 / CAM1_PWR#	Camera 1 Power Enable, active low output.	O CMOS 1.8V		Shared with GPIO1
		GPIO Pin 1 Preferred Output	I/O CMOS 1.8V	PU 470k	Alternative use: CAM1_PWR#
P110	GPIO2 / CAM0_RST#	Camera 0 reset, active low output	O CMOS 1.8V		Shared with GPIO2
		GPIO Pin 2 Preferred Output	I/O CMOS 1.8V	PU 470k	Alternative use: CAM0_RST#
P111	GPIO3 / CAM1_RST#	Camera 1 reset, active low output	O CMOS 1.8V		Shared with GPIO3
		GPIO Pin 3 Preferred Output	I/O CMOS 1.8V	PU 470k	Alternative use: CAM1_RST#
P112	GPIO4 / HDA_RST#	High Definition Audio Reset Output to Codec, low active.	O CMOS 1.8V / 1.5V		SMARC requires 1.5V or 1.8V HD Audio signaling. Please check with your Module vendor if 1.5V or 1.8V are supported and use an audio codec that is capable to support the regarding I/O voltage. The SMARC HD Audio pins are shared with

P-PIN	Primary	Description	Type	Termin-ation	Comment
					the I2S2 pins, which are defined to be 1.8V. This specification ignores the discrepancy between the 1.5V and 1.8V signaling, as the chance of damage in mismatched systems is negligible.
		GPIO Pin 4 Preferred Output	I/O CMOS 1.8V	PU 470k	Alternative use: HDA_RST#
P113	GPIO5 / PWM_OUT	GPIO Pin 5 Preferred Output	I/O CMOS 1.8V	PU 470k	Alternative use: PWM_OUT
		Fan Speed Control	O CMOS 1.8V	PU 470k	Uses the Pulse Width Modulation (PWM) technique to control the fan's RPM.
P114	GPIO6 / TACHIN	GPIO Pin 6 Preferred Input	I/O CMOS 1.8V	PU 470k	Alternative use: TACHIN
		Fan Tachometer Input	I CMOS 1.8V	PU 470k	
P115	GPIO7	GPIO Pin 7 Preferred Input	I/O CMOS 1.8V	PU 470k	
P116	GPIO8	GPIO Pin 8 Preferred Input	I/O CMOS 1.8V	PU 470k	
P117	GPIO9	GPIO Pin 9 Preferred Input	I/O CMOS 1.8V	PU 470k	
P118	GPIO10	GPIO Pin 10 Preferred Input	I/O CMOS 1.8V	PU 470k	
P119	GPIO11	GPIO Pin 11 Preferred Input	I/O CMOS 1.8V	PU 470k	
P120	GND				
P121	I2C_PM_CK	Power management I2C bus CLK	I/O OD CMOS 1.8V	PU 2k2	On x86 systems these serve as SMB CLK.
P122	I2C_PM_DAT	Power management I2C bus DATA	I/O OD CMOS 1.8V	PU 2k2	On x86 systems these serve as SMB DATA.
P123	BOOT_SEL0#	Input straps determine the Module boot device.	I OD CMOS 1.8V	PU 10k	Driven by OD on Carrier.
P124	BOOT_SEL1#	Input straps determine the Module boot device.	I OD CMOS 1.8V	PU 10k	Driven by OD on Carrier.
P125	BOOT_SEL2#	Input straps determine the Module boot device.	I OD CMOS 1.8V	PU 10k	Driven by OD on Carrier.
P126	RESET_OUT#	General purpose reset output to Carrier Board.	O CMOS 1.8V		
P127	RESET_IN#	Reset input from Carrier Board. Carrier drives low to force a Module reset, floats the line otherwise. This signal Shall be level triggered during bootup to allow to stop booting of the module. After bootup it May act as an edge triggered signal.	I OD CMOS 1.8 to 5 V	PU 10k	Driven by OD on Carrier.
P128	POWER_BTN#	Power-button input from Carrier Board. Carrier to float the line in in-active state. Active low, level sensitive. Should be debounced on the Module.	I OD CMOS 1.8 to 5 V	PU 10k	Driven by OD on Carrier.
P129	SER0_TX	Asynchronous Serial Data Output Port 0	O CMOS 1.8V		

P-PIN	Primary	Description	Type	Termination	Comment
P130	SER0_RX	Asynchronous Serial Data Input Port 0	I CMOS 1.8V	PU 100k	
P131	SER0_RTS#	Request to Send Handshake Line for Port 0	O CMOS 1.8V		
P132	SER0_CTS#	Clear to Send Handshake Line for Port 0	I CMOS 1.8V		
P133	GND				
P134	SER1_TX	Asynchronous Serial Data Output Port 1	O CMOS 1.8V		
P135	SER1_RX	Asynchronous Serial Data Input Port 1	I CMOS 1.8V	PU 100k	
P136	SER2_TX	Asynchronous Serial Data Output Port 2	O CMOS 1.8V		Not connected
P137	SER2_RX	Asynchronous Serial Data Input Port 2	I CMOS 1.8V		Not connected
P138	SER2_RTS#	Request to Send Handshake Line for Port 2	O CMOS 1.8V		Not connected
P139	SER2_CTS#	Clear to Send Handshake Line for Port 2	I CMOS 1.8V		Not connected
P140	SER3_TX	Asynchronous Serial Data Output Port 3	O CMOS 1.8V		
P141	SER3_RX	Asynchronous Serial Data Input Port 3	I CMOS 1.8V	PU 100k	
P142	GND				
P143	CAN0_TX	CAN Port 0 Transmit Output	O CMOS 1.8V		
P144	CAN0_RX	CAN Port 0 Receive Input	I CMOS 1.8V		
P145	CAN1_TX	CAN Port 1 Transmit Output	O CMOS 1.8V		
P146	CAN1_RX	CAN Port1 Receive Input	I CMOS 1.8V		
P147	VDD_IN	Module power input voltage - 3.3V min to 5.25V max	Analog 3.3V to 5.25V		
P148	VDD_IN	Module power input voltage - 3.3V min to 5.25V max	Analog 3.3V to 5.25V		
P149	VDD_IN	Module power input voltage - 3.3V min to 5.25V max	Analog 3.3V to 5.25V		
P150	VDD_IN	Module power input voltage - 3.3V min to 5.25V max	Analog 3.3V to 5.25V		
P151	VDD_IN	Module power input voltage - 3.3V min to 5.25V max	Analog 3.3V to 5.25V		
P152	VDD_IN	Module power input voltage - 3.3V min to 5.25V max	Analog 3.3V to 5.25V		
P153	VDD_IN	Module power input voltage - 3.3V min to 5.25V max	Analog 3.3V to 5.25V		
P154	VDD_IN	Module power input voltage - 3.3V min to 5.25V max	Analog 3.3V to 5.25V		
P155	VDD_IN	Module power input voltage - 3.3V min to 5.25V max	Analog 3.3V to 5.25V		
P156	VDD_IN	Module power input voltage - 3.3V min to 5.25V max	Analog 3.3V to 5.25V		

7.1.2. Pinout of SMARC Connector (Bottom Side)

Table 31: SMARC 2.1 Specification Pinout (bottom side)

S-Pin	Secondary	Description	Type	Termination	Comment
S1	CSI1_TX+ / I2C_CAM1_CK	I2C clock for serial camera data support link or differential data lane	I/O OD CMOS / O M-PHY 1.8V	PU 2.2K	Not Connected
S2	CSI1_TX- / I2C_CAM1_DAT	I2C data for serial camera data support link or differential data lane	I/O OD CMOS / O M-PHY 1.8V	PU 2.2K	Not Connected
S3	GND				
S4	RSVD				Not Connected
S5	CSI0_TX+ / I2C_CAM0_CK	I2C clock for serial camera data support link or differential data lane	I/O OD CMOS / O M-PHY 1.8V	PU 2.2K	Not Connected
S6	CAM_MCK				Not Connected
S7	CSI0_TX- / I2C_CAM0_DAT	I2C data for serial camera data support link or differential data lane	I/O ODvMOS / O M-PHY 1.8V	PU 2.2K	Not Connected
S8	CSI0_CK+	CSI0 differential clock input (point to point)	I D-PHY		Not Connected
S9	CSI0_CK-	CSI0 differential clock input (point to point)	I D-PHY		Not Connected
S10	GND				
S11	CSI0_RX0+	CSI0 differential input	I D-PHY / I M-PHY		Not Connected
S12	CSI0_RX0-	CSI0 differential input	I D-PHY / I M-PHY		Not Connected
S13	GND				
S14	CSI0_RX1+	CSI0 differential input	I D-PHY / I M-PHY		Not Connected
S15	CSI0_RX1-	CSI0 differential input	I D-PHY / I M-PHY		Not Connected
S16	GND				
S17	GBE1_MDI0+	Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations	I/O GBE MDI		Gigabit Ethernet Controller 1: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes. Some pairs are unused in some modes according to the following:
S18	GBE1_MDI0-	Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module	I/O GBE MDI		Gigabit Ethernet Controller 1: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.

	1000	100	10
MDI0 +/-	B1_DA+/-	TX+/-	TX+/-
MDI1 +/-	B1_DB+/-	RX+/-	RX+/-
MDI2 +/-	B1_DC+/-		
MDI3 +/-	B1_DD+/-		

<table>
<tr><th>S-Pin</th><th>Secondary</th><th>Description</th><th>Type</th><th>Termin-ation</th><th>Comment</th></tr>
<tr><td></td><td></td><td>appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations</td><td></td><td></td><td>Some pairs are unused in some modes according to the following:
<table>
<tr><td></td><td>1000</td><td>100</td><td>10</td></tr>
<tr><td>MDI0 +/-</td><td>B1_DA+/-</td><td>TX+/-</td><td>TX+/-</td></tr>
<tr><td>MDI1 +/-</td><td>B1_DB+/-</td><td>RX+/-</td><td>RX+/-</td></tr>
<tr><td>MDI2 +/-</td><td>B1_DC+/-</td><td></td><td></td></tr>
<tr><td>MDI3 +/-</td><td>B1_DD+/-</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>S19</td><td>GBE1_LINK100#</td><td>Link Speed Indication LED for GBE1 100Mbps</td><td>O OD CMOS 3.3V</td><td></td><td>Shall be able to sink 24mA or more Carrier LED current.</td></tr>
<tr><td>S20</td><td>GBE1_MDI1+</td><td>Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations</td><td>I/O GBE MDI</td><td></td><td>Gigabit Ethernet Controller 1:
Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.
Some pairs are unused in some modes according to the following:
<table>
<tr><td></td><td>1000</td><td>100</td><td>10</td></tr>
<tr><td>MDI0 +/-</td><td>B1_DA+/-</td><td>TX+/-</td><td>TX+/-</td></tr>
<tr><td>MDI1 +/-</td><td>B1_DB+/-</td><td>RX+/-</td><td>RX+/-</td></tr>
<tr><td>MDI2 +/-</td><td>B1_DC+/-</td><td></td><td></td></tr>
<tr><td>MDI3 +/-</td><td>B1_DD+/-</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>S21</td><td>GBE1_MDI1-</td><td>Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations</td><td>I/O GBE MDI</td><td></td><td>Gigabit Ethernet Controller 1:
Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.
Some pairs are unused in some modes according to the following:
<table>
<tr><td></td><td>1000</td><td>100</td><td>10</td></tr>
<tr><td>MDI0 +/-</td><td>B1_DA+/-</td><td>TX+/-</td><td>TX+/-</td></tr>
<tr><td>MDI1 +/-</td><td>B1_DB+/-</td><td>RX+/-</td><td>RX+/-</td></tr>
<tr><td>MDI2 +/-</td><td>B1_DC+/-</td><td></td><td></td></tr>
<tr><td>MDI3 +/-</td><td>B1_DD+/-</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>S22</td><td>GBE1_LINK1000#</td><td>Link Speed Indication LED for GBE1 1000Mbps</td><td>O OD CMOS 3.3V</td><td></td><td>Shall be able to sink 24mA or more Carrier LED current.</td></tr>
<tr><td>S23</td><td>GBE1_MDI2+</td><td>Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for</td><td>I/O GBE MDI</td><td></td><td>Gigabit Ethernet Controller 1:
Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.
Some pairs are unused in some modes according to the following:
<table>
<tr><td></td><td>1000</td><td>100</td><td>10</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>S-Pin</th><th>Secondary</th><th>Description</th><th>Type</th><th>Termin-ation</th><th>Comment</th></tr>
<tr><td></td><td></td><td>Gigabit Ethernet implementations</td><td></td><td></td><td>
<table>
<tr><td>MDI0 +/-</td><td>B1_D A+/-</td><td>TX+/ -</td><td>TX+/ -</td></tr>
<tr><td>MDI1 +/-</td><td>B1_D B+/-</td><td>RX+/ -</td><td>RX+/ -</td></tr>
<tr><td>MDI2 +/-</td><td>B1_D C+/-</td><td></td><td></td></tr>
<tr><td>MDI3 +/-</td><td>B1_D D+/-</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>S24</td><td>GBE1_MDI2-</td><td>Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations</td><td>I/O GBE MDI</td><td></td><td>Gigabit Ethernet Controller 1:
Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.
Some pairs are unused in some modes according to the following:
<table>
<tr><td></td><td>1000</td><td>100</td><td>10</td></tr>
<tr><td>MDI0 +/-</td><td>B1_D A+/-</td><td>TX+/ -</td><td>TX+/ -</td></tr>
<tr><td>MDI1 +/-</td><td>B1_D B+/-</td><td>RX+/ -</td><td>RX+/ -</td></tr>
<tr><td>MDI2 +/-</td><td>B1_D C+/-</td><td></td><td></td></tr>
<tr><td>MDI3 +/-</td><td>B1_D D+/-</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>S25</td><td>GND</td><td></td><td></td><td></td><td></td></tr>
<tr><td>S26</td><td>GBE1_MDI3+</td><td>Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations</td><td>I/O GBE MDI</td><td></td><td>Gigabit Ethernet Controller 1:
Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.
Some pairs are unused in some modes according to the following:
<table>
<tr><td></td><td>1000</td><td>100</td><td>10</td></tr>
<tr><td>MDI0 +/-</td><td>B1_D A+/-</td><td>TX+/ -</td><td>TX+/ -</td></tr>
<tr><td>MDI1 +/-</td><td>B1_D B+/-</td><td>RX+/ -</td><td>RX+/ -</td></tr>
<tr><td>MDI2 +/-</td><td>B1_D C+/-</td><td></td><td></td></tr>
<tr><td>MDI3 +/-</td><td>B1_D D+/-</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>S27</td><td>GBE1_MDI3-</td><td>Differential Pair Signals for External Transformer Carrier Series Termination: Magnetics Module appropriate for 10/100/1000 GBE transceivers Carrier Parallel Termination: Secondary side center tap terminations appropriate for Gigabit Ethernet implementations</td><td>I/O GBE MDI</td><td></td><td>Gigabit Ethernet Controller 1:
Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes.
Some pairs are unused in some modes according to the following:
<table>
<tr><td></td><td>1000</td><td>100</td><td>10</td></tr>
<tr><td>MDI0 +/-</td><td>B1_D A+/-</td><td>TX+/ -</td><td>TX+/ -</td></tr>
<tr><td>MDI1 +/-</td><td>B1_D B+/-</td><td>RX+/ -</td><td>RX+/ -</td></tr>
<tr><td>MDI2 +/-</td><td>B1_D C+/-</td><td></td><td></td></tr>
</table>
</td></tr>
</table>

S-Pin	Secondary	Description	Type	Termination	Comment
					MDI3 +/- | B1_DD+/- |	
S28	GBE1_CTREF	Center-Tap Reference Voltage for Carrier Board Ethernet Magnetic (if required by the Module GBE PHY)	Analog 0 to 3.3V max		
S29	PCIE_D_TX+ / SERDES_0_TX+	Differential PCIe link D transmit data pair	O PCIE		Series AC coupled on Module 75-265nF depending on PCIe generation
		Differential SERDES 0 Transmit Data Pair	O PCIE		Series AC coupled on Module
S30	PCIE_D_TX- / SERDES_0_TX-	Differential PCIe link D transmit data pair	O PCIE		Series AC coupled on Module 75-265nF depending on PCIe generation
		Differential SERDES 0 Transmit Data Pair	O PCIE		Series AC coupled on Module
S31	GBE1_LINK_ACT#	Link / Activity Indication LED Driven Low on Link (10, 100 or 1000 Mbps) Blinks on Activity	O OD CMOS 3.3V		Shall be able to sink 24mA or more Carrier LED current.
S32	PCIE_D_RX+ / SERDES_0_RX+	Differential PCIe link D receive data pair	I PCIE		Series AC coupled off Module 75-265nF depending on PCIe generation
		Differential SERDES 0 Receive Data Pair	I PCIE		Series AC coupled on Carrier
S33	PCIE_D_RX- / SERDES_0_RX-	Differential PCIe link D receive data pair	I PCIE		Series AC coupled off Module 75-265nF depending on PCIe generation
		Differential SERDES 0 Receive Data Pair	I PCIE		Series AC coupled on Carrier
S34	GND				
S35	USB4+	USB Differential Data Pairs for Port 4	I/O USB		
S36	USB4-	USB Differential Data Pairs for Port 4	I/O USB		
S37	USB3_VBUS_DET	USB Port 3 Host Power Detection	I USB VBUS 5V		when this Port is used as a Device
S38	AUDIO_MCK	Master Clock Output to I2S Codec(s)	O CMOS 1.8V		
S39	I2S0_LRCK	I2S0 Left & Right Synchronization Clock	I/O CMOS 1.8V		Module Output if CPU acts in Master Mode. Module Input if CPU acts in Slave Mode
S40	I2S0_SDOUT	I2S0 Digital Audio Output	O CMOS 1.8V		
S41	I2S0_SDIN	I2S0 Digital Audio Input	I CMOS 1.8V		
S42	I2S0_CK	I2S0 Digital Audio Clock	I/O CMOS 1.8V		Module Output if CPU acts in Master Mode Module Input if CPU acts in Slave Mode
S43	ESPI_ALERT0#	ESPI ALERT	I OD CMOS 1.8V	PU 4.7k	These pins are used by eSPI slaves to request service from eSPI master. Open-drain output from the slave. This pin is optional for Single Master-Single Slave configuration where I/O[1] can be used to signal the Alert event
S44	ESPI_ALERT1#	ESPI ALERT	I OD CMOS 1.8V	PU 4.7k	These pins are used by eSPI slaves to request service from eSPI master. Open-drain output from the slave. This pin is optional for Single Master-Single Slave

S-Pin	Secondary	Description	Type	Termin-ation	Comment
					configuration where I/O[1] can be used to signal the Alert event
S45	MDIO_CLK	MDIO Signals to Configure Possible PHYs	O CMOS 1.8V		Signal for communication to a PHY
S46	MDIO_DAT	MDIO Signals to Configure Possible PHYs	I/O OD CMOS 1.8V	PU 1k5	Signal for communication to a PHY
S47	GND				
S48	I2C_GP_CK	General Purpose I2C Clock Signal	I/O OD CMOS 1.8V	PU 2k2	
S49	I2C_GP_DAT	General Purpose I2C Data Signal	I/O OD CMOS 1.8V	PU 2k2	
S50	HDA_SYNC / I2S2_LRCK	High Definition Audio Sample synchronization clock to codec	I/O CMOS 1.8V / 1.5V		SMARC requires 1.5V or 1.8V HD Audio signaling. Please check with your Module vendor if 1.5V or 1.8V are supported and use an audio codec that is capable to support the regarding I/O voltage. The SMARC HD Audio pins are shared with the I2S2 pins, which are defined to be 1.8V. This specification ignores the discrepancy between the 1.5V and 1.8V signaling, as the chance of damage in mismatched systems is negligible.
		I2S2 Left & Right Synchronization Clock	I/O CMOS 1.8V		Module Output if CPU acts in Master Mode. Module Input if CPU acts in Slave Mode
S51	HDA_SDO / I2S2_SDOUT	High Definition Audio data out to codec	O CMOS 1.8V / 1.5V		SMARC requires 1.5V or 1.8V HD Audio signaling. Please check with your Module vendor if 1.5V or 1.8V are supported and use an audio codec that is capable to support the regarding I/O voltage. The SMARC HD Audio pins are shared with the I2S2 pins, which are defined to be 1.8V. This specification ignores the discrepancy between the 1.5V and 1.8V signaling, as the chance of damage in mismatched systems is negligible.
		I2S2 Digital Audio Output	O CMOS 1.8V		
S52	HDA_SDI / I2S2_SDIN	High Definition Audio data in from codec"	I/O CMOS 1.8V / 1.5V		SMARC requires 1.5V or 1.8V HD Audio signaling. Please check with your Module vendor if 1.5V or 1.8V are supported and use an audio codec that is capable to support the regarding I/O voltage. The SMARC HD Audio pins are shared with the I2S2 pins, which are defined to be 1.8V. This specification ignores the discrepancy between the 1.5V and 1.8V signaling, as the chance of damage in mismatched systems is negligible.
		I2S2 Digital Audio Input	I CMOS 1.8V		
S53	HDA_CK / I2S2_CK	High Definition Audio clock to codec	O CMOS 1.8V / 1.5V		SMARC requires 1.5V or 1.8V HD Audio signaling. Please check with your Module vendor if 1.5V or 1.8V are supported and use an audio codec that is capable to support the regarding I/O voltage. The SMARC HD Audio pins are shared with the I2S2 pins, which are defined to be 1.8V. This specification ignores the

S-Pin	Secondary	Description	Type	Termin-ation	Comment
					discrepancy between the 1.5V and 1.8V signaling, as the chance of damage in mismatched systems is negligible.
		I2S2 Digital Audio Clock	I/O CMOS 1.8V		Module Output if CPU acts in Master Mode. Module Input if CPU acts in Slave Mode
S54	SATA_ACT#	SATA Activity Indicator	O OD CMOS 3.3V		Shall be able to sink 24mA or more Carrier LED current
S55	USB5_EN_OC#	USB Over-Current Sense for Port 5	I/O OD CMOS 3.3V	PU 10k	Pulled low by Module OD driver to disable USB5 power. Pulled low by Carrier OD driver to indicate over-current situation.
S56	ESPI_IO_2 / QSPI_IO_2	ESPI Master Data Input / Output	I/O CMOS 1.8V		In Single I/O mode, ESPI_IO_0 is the eSPI master output / eSPI slave input (MOSI) whereas ESPI_IO_1 is the SPI master input / eSPI slave output (MISO).
		QSPI Data input / output	I/O CMOS 1.8V		
S57	ESPI_IO_3 / QSPI_IO_3	ESPI Master Data Input / Output	I/O CMOS 1.8V		In Single I/O mode, ESPI_IO_0 is the eSPI master output / eSPI slave input (MOSI) whereas ESPI_IO_1 is the SPI master input / eSPI slave output (MISO).
		QSPI Data input / output	I/O CMOS 1.8V		
S58	ESPI_RESET#	ESPI Reset	O CMOS 1.8V		Reset the eSPI interface for both master and slaves.eSPI Reset# is typically driven from eSPI master to eSPI slaves
S59	USB5+	USB Differential Data Pairs for Port 5	I/O USB		
S60	USB5-	USB Differential Data Pairs for Port 5	I/O USB		
S61	GND				
S62	USB3_SSTX+	Transmit Signal Differential Pairs for SuperSpeed on Port 3	O USB SS		DC blocking capacitors 100nF ***shall*** be placed on the Module
S63	USB3_SSTX-	Transmit Signal Differential Pairs for SuperSpeed on Port 3	O USB SS		DC blocking capacitors 100nF ***shall*** be placed on the Module
S64	GND				
S65	USB3_SSRX+	Receive Signal Differential Pairs for SuperSpeed on Port 3	I USB SS		DC blocking capacitors 100nF ***shall*** be placed on the Carrier
S66	USB3_SSRX-	Receive Signal Differential Pairs for SuperSpeed on Port 3	I USB SS		DC blocking capacitors 100nF ***shall*** be placed on the Carrier
S67	GND				
S68	USB3+	USB Differential Data Pairs for Port 3	I/O USB		
S69	USB3-	USB Differential Data Pairs for Port 3	I/O USB		
S70	GND				
S71	USB2_SSTX+	Transmit Signal Differential Pairs for SuperSpeed on Port 2	O USB SS		DC blocking capacitors 100nF shall be placed on the Module

S-Pin	Secondary	Description	Type	Termination	Comment
S72	USB2_SSTX-	Transmit Signal Differential Pairs for SuperSpeed on Port 2	O USB SS		DC blocking capacitors 100nF ***shall*** be placed on the Module
S73	GND				
S74	USB2_SSRX+	Receive Signal Differential Pairs for SuperSpeed on Port 2	I USB SS		DC blocking capacitors 100nF ***shall*** be placed on the Carrier
S75	USB2_SSRX-	Receive Signal Differential Pairs for SuperSpeed on Port 2	I USB SS		DC blocking capacitors 100nF ***shall*** be placed on the Carrier
S76	PCIE_B_RST#	PCIe Port B reset output	O CMOS 3.3V		
S77	PCIE_C_RST#	PCIe Port C reset output	O CMOS 3.3V		
S78	PCIE_C_RX+ / SERDES_1_RX+	Differential PCIe link C receive data pair	I PCIE		Series AC coupled off Module 75-265nF depending on PCIe generation
		Differential SERDES 1 Receive Data Pair	I PCIE		Series AC coupled on Carrier
S79	PCIE_C_RX- / SERDES_1_RX-	Differential PCIe link C receive data pair	I PCIE		Series AC coupled off Module 75-265nF depending on PCIe generation
		Differential SERDES 1 Receive Data Pair	I PCIE		Series AC coupled on Carrier
S80	GND				
S81	PCIE_C_TX+ / SERDES_1_TX+	Differential PCIe link C transmit data pair	O PCIE		Series AC coupled on Module 75-265nF depending on PCIe generation
		Differential SERDES 1 Transmit Data Pair	O PCIE		Series AC coupled on Module
S82	PCIE_C_TX- / SERDES_1_TX-	Differential PCIe link C transmit data pair	O PCIE		Series AC coupled on Module 75-265nF depending on PCIe generation
		Differential SERDES 1 Transmit Data Pair	O PCIE		Series AC coupled on Module
S83	GND				
S84	PCIE_B_REFCK+	Differential PCIe Link B reference clock output	O PCIE		
S85	PCIE_B_REFCK-	Differential PCIe Link B reference clock output	O PCIE		
S86	GND				
S87	PCIE_B_RX+	Differential PCIe link B receive data pair	I PCIE		Series AC coupled off Module 75-265nF depending on PCIe generation
S88	PCIE_B_RX-	Differential PCIe link B receive data pair	I PCIE		Series AC coupled off Module 75-265nF depending on PCIe generation
S89	GND				
S90	PCIE_B_TX+	Differential PCIe link B transmit data pair	O PCIE		Series AC coupled on Module 75-265nF depending on PCIe generation
S91	PCIE_B_TX-	Differential PCIe link B transmit data pair	O PCIE		Series AC coupled on Module 75-265nF depending on PCIe generation
S92	GND				
S93	DP0_LANE0+	Primary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
S94	DP0_LANE0-	Primary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier

S-Pin	Secondary	Description	Type	Termination	Comment
S95	DP0_AUX_SEL	Auxiliary Selection	I CMOS 1.8V	PD 1M	Pulled to GND on Carrier for DP operation in Dual Mode (DP++) implementations Module must tolerate high level in stand-by mode. Should be connected to pin 13 of the DisplayPort connector to enable a dual-mode DisplayPort interface.
S96	DP0_LANE1+	Primary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
S97	DP0_LANE1-	Primary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
S98	DP0_HPD	DP Hot Plug Detect Input	I CMOS 1.8V	PD 1M	Module must tolerate high level in stand-by mode. The Carrier shall include a blocking FET on DP[0:1]_HPD to prevent back-drive current from damaging the Module.
S99	DP0_LANE2+	Primary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
S100	DP0_LANE2-	Primary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
S101	GND				
S102	DP0_LANE3+	Primary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
S103	DP0_LANE3-	Primary DP Port Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier
S104	USB3_OTG_ID	Input Pin to Announce OTG Device Insertion on USB 3.2 Port	I CMOS 3.3V		
S105	DP0_AUX+	Primary DP Port Bidirectional Channel used for Link Management and Device Control	I/O DP 3.3V	PD 100k	AC coupled on Module. If DP0_AUX_SEL=0 (DP mode): AC coupled on module, 100k PD. If DP0_AUX_SEL=1 (HDMI mode): DC coupled, CMOS, 100k PU. In case of HDMI over DP++ implementation, stronger pull-up is demanded to the Carrier Board.
S106	DP0_AUX-	Primary DP Port Bidirectional Channel used for Link Management and Device Control	I/O DP 3.3V	PU 100k	AC coupled on Module. If DP0_AUX_SEL=0 (DP mode): AC coupled on module, 100k PU. If DP0_AUX_SEL=1 (HDMI mode): DC coupled, CMOS, 100k PU. In case of HDMI over DP++ implementation, stronger pull-up is demanded to the Carrier Board.
S107	LCD1_BKLT_EN	Secondary LVDS Channel Backlight Enable	O CMOS 1.8V		Active high Only in use, when two separate LVDS ports are supported.
		Secondary Panel Backlight Enable	O CMOS 1.8V		Active high Only in use, when two separated eDP ports are supported.
		Secondary Panel Backlight Enable	O CMOS 1.8V		Active high
S108	LVDS1_CK+ / eDP1_AUX+ / DSI1_CLK+	Secondary LVDS Channel Differential Pair Clock Lines	O LVDS		100 ohm differential termination across the differential pair at the endpoint of the signal path, usually on the display assembly.
		Secondary Bidirectional Channel used for Link Management and Device Control	I/O DP		AC coupled off Module -only in use, when two separate eDP ports are supported.

S-Pin	Secondary	Description	Type	Termination	Comment
		Secondary DSI Panel Differential Pair Clock Lines	O D-PHY		
S109	LVDS1_CK- / eDP1_AUX- / DSI1_CLK-	Secondary LVDS Channel Differential Pair Clock Lines	O LVDS		100 ohm differential termination across the differential pair at the endpoint of the signal path, usually on the display assembly.
		Secondary Bidirectional Channel used for Link Management and Device Control	I/O DP		AC coupled off Module -only in use, when two separate eDP ports are supported.
		Secondary DSI Panel Differential Pair Clock Lines	O D-PHY		
S110	GND				
S111	LVDS1_0+ / eDP1_TX0+ / DSI1_D0+	Secondary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Secondary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier. Only in use, when two separate eDP ports are supported.
		Secondary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S112	LVDS1_0- / eDP1_TX0- / DSI1_D0-	Secondary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Secondary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier. Only in use, when two separate eDP ports are supported.
		Secondary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S113	eDP1_HPD / DSI1_TE	Detection of Hot Plug / Unplug of Secondary eDP Display and Notification of the Link Layer	I CMOS 1.8V	PD 1M	Only in use, when two separated eDP ports are supported. Please check Module user guide! Module must tolerate high level in stand-by mode
		Secondary DSI Panel Tearing Effect Signal	I CMOS 1.8V	PD 1M	
S114	LVDS1_1+ / eDP1_TX1+ / DSI1_D1+	Secondary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Secondary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier. Only in use, when two separate eDP ports are supported.
		Secondary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S115	LVDS1_1- / eDP1_TX1- / DSI1_D1-	Secondary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.

S-Pin	Secondary	Description	Type	Termination	Comment
		Secondary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier. Only in use, when two separate eDP ports are supported.
		Secondary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S116	LCD1_VDD_EN	Secondary LVDS Channel Power Enable	O CMOS 1.8V		Active high Only in use, when two separate LVDS ports are supported.
		Secondary Panel Power Enable	O CMOS 1.8V		Active high Only in use, when two separated eDP ports are supported.
		Secondary Panel Power Enable	O CMOS 1.8V		Active high
S117	LVDS1_2+ / eDP1_TX2+ / DSI1_D2+	Secondary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Secondary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier. Only in use, when two separate eDP ports are supported.
		Secondary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S118	LVDS1_2- / eDP1_TX2- / DSI1_D2-	Secondary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Secondary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier. Only in use, when two separate eDP ports are supported.
		Secondary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S119	GND				
S120	LVDS1_3+ / eDP1_TX3+ / DSI1_D3+	Secondary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Secondary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier. Only in use, when two separate eDP ports are supported.
		Secondary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S121	LVDS1_3- / eDP1_TX3- / DSI1_D3-	Secondary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Secondary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier. Only in use, when two separate eDP ports are supported.

S-Pin	Secondary	Description	Type	Termination	Comment
		Secondary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S122	LCD1_BKLT_PWM	Secondary LVDS Channel Brightness Control	O CMOS 1.8V		Through pulse width modulation (PWM) only in use, when two separate LVDS ports are supported.
		Secondary Panel Brightness Control	O CMOS 1.8V		Through Pulse Width Modulation (PWM) Only in use, when two separated eDP ports are supported.
		Secondary Panel Brightness Control	O CMOS 1.8V		Through pulse width modulation (PWM)
S123	GPIO13	GPIO Pin 13 Preferred Input	I/O CMOS 1.8V	PU 470k	
S124	GND				
S125	LVDS0_0+ / eDP0_TX0+ / DSI0_D0+	Primary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Primary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier.
		Primary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S126	LVDS0_0- / eDP0_TX0- / DSI0_D0-	Primary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Primary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier.
		Primary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S127	LCD0_BKLT_EN	Primary LVDS Channel Backlight Enable	O CMOS 1.8V		Active high
		Primary Panel Backlight Enable	O CMOS 1.8V		Active high
		Primary Panel Backlight Enable	O CMOS 1.8V		Active high
S128	LVDS0_1+ / eDP0_TX1+ / DSI0_D1+	Primary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Primary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier.
		Primary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S129	LVDS0_1- / eDP0_TX1- / DSI0_D1-	Primary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Primary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier.

S-Pin	Secondary	Description	Type	Termination	Comment
		Primary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S130	GND				
S131	LVDS0_2+ / eDP0_TX2+ / DSI0_D2+	Primary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Primary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier.
		Primary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S132	LVDS0_2- / eDP0_TX2- / DSI0_D2-	Primary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Primary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier.
		Primary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S133	LCD0_VDD_EN	Primary LVDS Channel Power Enable	O CMOS 1.8V		Active high
		Primary Panel Power Enable	O CMOS 1.8V		Active high
		Primary Panel Power Enable	O CMOS 1.8V		Active high
S134	LVDS0_CK+ / eDP0_AUX+ / DSI0_CLK+	Primary LVDS Channel Differential Pair Clock Lines	O LVDS		100 ohm differential termination across the differential pair at the endpoint of the signal path, usually on the display assembly.
		Primary Bidirectional Channel used for Link Management and Device Control	I/O DP		AC coupled off Module
		Primary DSI Panel Differential Pair Clock Lines	O D-PHY		
S135	LVDS0_CK- / eDP0_AUX- / DSI0_CLK-	Primary LVDS Channel Differential Pair Clock Lines	O LVDS		100 ohm differential termination across the differential pair at the endpoint of the signal path, usually on the display assembly.
		Primary Bidirectional Channel used for Link Management and Device Control	I/O DP		AC coupled off Module
		Primary DSI Panel Differential Pair Clock Lines	O D-PHY		
S136	GND				
S137	LVDS0_3+ / eDP0_TX3+ / DSI0_D3+	Primary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Primary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier.
		Primary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.

S-Pin	Secondary	Description	Type	Termination	Comment
S138	LVDS0_3- / eDP0_TX3- / DSI0_D3-	Primary LVDS Channel Differential Pair Data Lines	O LVDS		100 ohm differential termination across the differential pairs at the endpoint of the signal path, usually on the display assembly.
		Primary 4-Lane eDP Differential Pair Data Lines	O DP		AC coupled off Module 100nF DC blocking capacitors shall be placed on the Carrier.
		Primary DSI Panel Differential Pair Data Lines	O D-PHY		No blocking capacitors or termination required. Layout for 90 ohm differential impedance.
S139	I2C_LCD_CK	DDC Clock Line Used for Flat Panel Detection and Control	I/O OD CMOS 1.8V	PU 2k2	Possible conflict if two LVDS panels are used
		I2C clock to read LCD display EDID EEPROMs	I/O OD CMOS 1.8V	PU 2k2	Optional - eDP panel information is usually exchanged via the eDP auxiliary pair
		DDC Clock Line Used for Flat Panel Detection and Control	I/O OD CMOS 1.8V	PU 2k2	Possible conflict if two LVDS panels are used
S140	I2C_LCD_DAT	DDC Data Line Used for Flat Panel Detection and Control	I/O OD CMOS 1.8V	PU 2k2	Possible conflict if two LVDS panels are used
		I2C Data to Read LCD Display EDID EEPROMs	I/O OD CMOS 1.8V	PU 2k2	Possible EDID EEPROM Address conflicts may occur if multiple displays are implemented Optional - eDP panel information is usually exchanged via the eDP auxiliary pair
		DDC Data Line Used for Flat Panel Detection and Control	I/O OD CMOS 1.8V	PU 2k2	Possible conflict if two LVDS panels are used
S141	LCD0_BKLT_PWM	Primary LVDS Channel Brightness Control	O CMOS 1.8V		Through Pulse Width Modulation (PWM)
		Primary Panel Brightness Control	O CMOS 1.8V		Through pulse width modulation (PWM)
		Primary Panel Brightness Control	O CMOS 1.8V		Through pulse width modulation (PWM)
S142	GPIO12	GPIO Pin 12 Preferred Input	I/O CMOS 1.8V	PU 470k	
S143	GND				
S144	eDP0_HPD / DSI0_TE	Detection of Hot Plug / Unplug of Primary eDP Display and Notification of the Link Layer	I CMOS 1.8V	PD 1M	Module must tolerate high level in stand-by mode
		Primary DSI Panel Tearing Effect Signal	I CMOS 1.8V	PD 1M	
S145	WDT_TIME_OUT#	Watch-Dog-Timer Output, low active	O CMOS 1.8V		
S146	PCIE_WAKE#	PCIe wake up interrupt to host – common to PCIe links A, B, C, D	I OD CMOS 3.3V	PU 10k	
S147	VDD_RTC	Low current RTC circuit backup power – 3.0V nominal.	Analog 2.0V to 3.25V		May be sourced from a carrier based lithium cell or super cap.
S148	LID#	Lid open/close indication to Module. Low indicates lid closure (which system may use to initiate a sleep state). Carrier to float the line in in-active state. Active low, level	I OD CMOS 1.8 to 5V	PU 10k	Driven by OD on Carrier.

S-Pin	Secondary	Description	Type	Termination	Comment
		sensitive. Should be de-bounced on the Module.			
S149	SLEEP#	Sleep indicator from Carrier Board. ***May*** be sourced from user Sleep button or Carrier logic. Carrier to float the line in in-active state. Active low, level sensitive. ***Should*** be de-bounced on the Module.	I OD CMOS 1.8 to 5V	PU 10k	Driven by OD on Carrier.
S150	VIN_PWR_BAD#	Power bad indication from Carrier Board. Module and Carrier power supplies (other than Module and Carrier power supervisory circuits) ***shall not*** be enabled while this signal is held low by the Carrier.	I OD CMOS VDD_IN	PU 10k	Module must implement PU but actual value is depended on particular Module design. Driven by OD on Carrier
S151	CHARGING#	Held low by Carrier during battery charging. Carrier to float the line when charge is complete.	I OD CMOS 1.8 to 5V	PU 10k	Driven by OD on Carrier.
S152	CHARGER_PRSNT#	Held low by Carrier if DC input for battery charger is present.	I OD CMOS 1.8 to 5V	PU 10k	Driven by OD on Carrier.
S153	CARRIER_STBY#	The Module ***shall*** drive this signal low when the system is in a standby power state.	O CMOS 1.8V		On x86 designs this pin should utilize the SUS_S3# signal.
S154	CARRIER_PWR_ON	Carrier Board circuits (apart from power management and power path circuits) ***should not*** be powered up until the Module asserts the CARRIER_PWR_ON signal.	O CMOS 1.8V		On x86 designs this pin should utilize a standby related power signal i.e. RSM_RST# or SLP_A# signal.
S155	FORCE_RECOV#	Low on this pin allows non-protected segments of Module boot device to be rewritten / restored from an external USB Host on Module USB0. The Module USB0 operates in Client Mode when in the Force Recovery function is invoked. Pulled high on the Module. For SOCs that do not implement a USB based Force Recovery functions, then a low on the Module FORCE_RECOV# pin may invoke the SOC native Force Recovery mode – such as over a Serial Port. For x86 systems this signal may be used to load BIOS defaults. Pulled up on Module. Driven by OD part on Carrier.	I OD CMOS 1.8V	PU 10k	Driven by OD on Carrier.
S156	BATLOW#	Battery low indication to Module. Carrier to float the line in inactive state.	I OD CMOS 1.8 to 5V	PU 10k	Driven by OD on Carrier.

S-Pin	Secondary	Description	Type	Termin-ation	Comment
S157	TEST#	Held Low by Carrier to Invoke Module Vendor Specific Test Functions	I OD CMOS 1.8 to 5V	PU vendor specific value	Module must implement PU but actual value is depended on particular Module design. Carrier Board should leave this pin floating for normal operation. Driven by OD on Carrier
S158	GND				

8/ Configuration

8.1. Boot Select

The three pins (BOOT_SEL2# Pin-P125; BOOT_SEL1# pin-P124; BOOT_SEL0#, pin-P123) determine the module's boot device. The pins are set to be either not connected (Float or pulled to ground), to select the required boot method.

Register for Kontron's Customer Section to get access to BIOS downloads and PCN service.

The SPI interface may only be used with a SPI Flash device to boot from the external BIOS on the carrier board.

Table 32: Boot Select

Carrier Connection			Boot Source
BOOT_SEL2#	BOOT_SEL1#	BOOT_SEL0#	
GND	GND	GND	NA
GND	GND	Float	NA
GND	Float	GND	NA
GND	Float	Float	Carrier SPI (CS0#)
Float	GND	GND	NA
Float	GND	Float	NA
Float	Float	GND	NA
Float	Float	Float	Module SPI

Booting takes place either from the on-module SPI Flash chip or the external SPI Flash chip on the carrier board.

8.1.1. Booting the SPI Flash

Initially, the EFI Shell is booted with an USB key containing the binary used to flash the module SPI Flash chip. To program the external SPI Flash chip on the carrier board with the BIOS binary, use an external programmer.

Visit Kontron's Customer Section to get access to BIOS downloads and PCN service.

To boot either the carrier board or module SPI flash chip, perform the following:

1. Connect a SPI flash with the correct size (similar to BIOS binary (*.BIN) file size) to the carrier SPI interface.

The external SPI flash chip on the carrier is required to be 32MByte (256MBit).

2. Open pin P123 (**BOOT_SEL0#**) and pin P124 (**BOOT_SEL1#**) and connect pin P125 (**BOOT_SEL2#**) to ground to enable the external SPI Flash chip to boot on carrier SPI or open pin P123 (**BOOT_SEL0#**) and pin P124 (**BOOT_SEL1#**) and pin P125 (**BOOT_SEL2#**) to enable SPI Flash chip to boot on-module SPI.

The command line is "EtaAfuOemEfi64".
BIOS file name: sXELRxxx.bin /b /p /n /x /me /r (xxx = version number)
In case of change, check Kontron's Customer Section for the latest BIOS binary package with reference command line.

8.2. Watch Dog

The watchdog timer interrupt is a hardware or software timer implemented by the module to the carrier board if there is a fault condition in the main program; the watchdog triggers a system reset or other corrective actions after a specific time, with the aim to bring the system back from a non-responsive to normal state.

The watchdog time-out event offers a signal that can be asserted when a watchdog timer has not been triggered within a set time. The WDT signal is configurable to any of the two stages. After reset, the signal is automatically deasserted. If deassertion is necessary during runtime, contact Kontron Support for further help.

Table 33: Dual Staged Watchdog Timer- Time-Out Events

0000b	**No action**	Stage is off and will be skipped
0001b	**Reset**	Restarts the module and starts a new POST and operating system
0101b	**Delay -> No action**	Might be necessary when an operating system must be started and the time for the first trigger pulse must be extended. Only available in the first stage!
1000b	**WDT Only**	Triggers WDT pin on the carrier board connector
1001b	**Reset + WDT**	
1101b	**DELAY + WDT -> No action**	

8.2.1. Watchdog Timer Signal

The watchdog interrupt (WDT_TIME_OUT#) on the SMARC® connector pin-S145 indicates a Watchdog time-out event. The WDT_TIME_OUT# signal is configurable to any of the two stages. For more details, contact Kontron Support.

8.3. Power Management

The SMARC-sXEL implements the Advanced Configuration and Power Interface (ACPI) 6.0 hardware specification with features such as power button and suspend states. The Power management options are available within the BIOS set up menu.

8.3.1. Suspend States

Supported ACPI suspend-states:

- Suspend to RAM (S3)
- Suspend-to-Disk (S4)
- Soft-off state (S5)

The module starts automatically after powered up to state S0. There is one bit in the NVM where this automatism can be changed. If the bit is changed the module stays in state S5 until a power up event occurred.

If power is removed, the wake-up event (S0) requires VDD_IN to power on the module.

8.3.2. Power Button (POWER_BTN#)

The power button (Pin-P128) is available through the SMARC connector. To start the module using the Power Button the PWRBTN# signal must be at least 50 ms (50 ms ≤ t < 4 s, typical 400 ms) at low level (Power Button Event).

Pressing the power button for at least 4 seconds turns off power to the module (Power Button Override)

8.3.3. Power Management Signals

The power supply control settings are set in the BIOS and enable the module to shut down, rest and wake from standby properly.

Table 34: Power Management Pins

SMARC Signal	SMARC Pin	Description
CARRIER_PWR_ON	S154	Carrier Board circuits (apart from power management and power path circuits) should not be powered up until the Module asserts the CARRIER_PWR_ON signal.
CARRIER_STBY#	S153	Module drives this signal low when the system is in a standby power state
CHARGER_PRSNT#	S152	Held low by Carrier if DC input for battery charger is present.
Charging#	S151	Held low by Carrier during battery charging. Carrier to float the line when charge is complete.
POWER_BTN#	P128	Power-button input from Carrier Board. Carrier to float the line in in-active state. Active low, level sensitive. Should be debounced on the Module.
LID#	S148	Lid open/close indication to Module. Low indicates lid closure (which system may use to initiate a sleep state). Carrier to float the line in inactive state. Active low, level sensitive. Should be de-bounced on the Module.
SLEEP#	S149	Sleep indicator from Carrier Board. May be sourced from user Sleep button or Carrier logic. Carrier to float the line in in-active state. Active low, level sensitive. Should be debounced on the Module
RESET_OUT#	P126	General purpose reset output to Carrier Board
RESET_IN#	P127	Reset input from Carrier Board. Carrier drives low to force a Module reset, floats the line otherwise. This signal is level triggered during bootup stop booting of the module. After bootup it acts as an edge triggered signal.
VIN_PWR_BAD#	S150	Power bad indication from Carrier Board. Module and Carrier power supplies (other than Module and Carrier power supervisory circuits) are not be enabled while this signal is held low by the Carrier.
BATLOW#	S156	Battery low indication to Module. Carrier to float the line in inactive state.
I2C_PM_DAT	P122	Power management I2C bus DATA
I2C_PM_CK	P121	Power management I2C bus CLK
SMB_ALERT#	P1	SMBus Alert# (Interrupt) Signal
TEST#	S157	Held Low by Carrier to Invoke Module Vendor Specific Test Functions

9/ uEFI BIOS

9.1. Starting the uEFI BIOS

The board is provided with a Kontron-customized, pre-installed and configured version of American Megatrends, Inc. (AMI). It is based on the Unified Extensible Firmware Interface (uEFI) specification and the Intel® Platform Innovation Framework for EFI. This uEFI BIOS provides a variety of new and enhanced functions specifically tailored to the hardware features of the SMARC-sXEL

The BIOS version covered in this document may not be the latest version. The latest version may have differences to the BIOS options and features described in this chapter.

Register for Kontron's Customer Section to get access to BIOS downloads and PCN service.

The uEFI BIOS comes with a Setup program which provides quick and easy access to the individual function settings for control or modification of the uEFI BIOS configuration. The Setup program allows the accessing of various menus which provide functions or access to sub-menus with more specific functions of their own.

To start the uEFI BIOS Setup program, follow the steps below:

1. Power on the board.
2. Wait until the first characters appear on the screen (POST messages or splash screen).
3. Press the <DEL> key.
4. If the uEFI BIOS is password-protected, a request for password will appear. Enter either the User Password or the Supervisor Password (see Security menu), press <RETURN>, and proceed with step 5.
5. A Setup menu appears.

9.2. Navigating the uEFI BIOS

The uEFI BIOS Setup program uses a hot key-based navigation system. A hot key legend bar is located on the bottom of the Setup screens. The following table provides information concerning the usage of these hot keys.

Table 35: Navigation Hot Keys Available in the Legend Bar

Hot Keys	Description
<F1>	The <F1> key is used to invoke the General Help window.
<->	The<Minus> key is used to select the next lower value within a field.
<+>	The <Plus> key is used to select the next higher value within a field.
<F4>	The <F4> key is used to Exit saving Changes.
<F3>	The key is used to load Optimized Defaults
<→> or <←>	The <Left/Right> arrows are used to select major Setup menus on the menu bar. For example: Main screen, Advanced screen, Security screen, etc.
<↑> or <↓>	The <Up/Down> arrows are used to select fields in the current menu. For example a Setup function or a sub-screen
<ESC>	The <ESC> key is used to exit a Setup menu
<RETURN>	The <RETURN> key is used to execute a command or select a submenu

9.3. Setup Menus

The Setup utility features a selection bar at the top of the screen that lists the available menus:

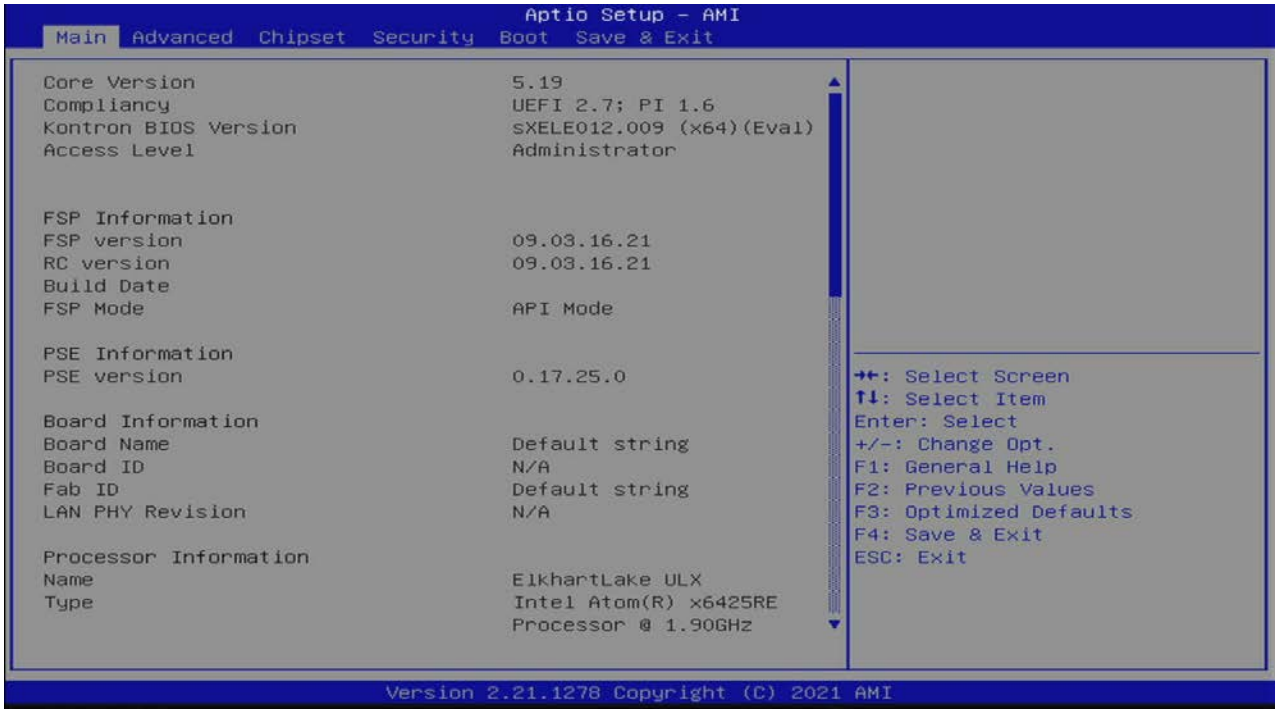
- Main
- Advanced
- Chipset
- Security
- Boot
- Save & Exit

The currently active menu and the currently active uEFI BIOS Setup item are highlighted in white. Use the left and right arrow keys to select the Setup menus. Each Setup menu provides two main frames. The left frame displays all available functions. Configurable functions are displayed in blue. Functions displayed in black provide information about the status or the operational configuration. The right frame displays a Help window providing an explanation of the respective function.

9.4. Main Setup Menu

On entering the uEFI BIOS, the Setup program displays the Main Setup menu. This screen lists basic system and board information.

Figure 16: Main Setup Menu



The following table shows the Main Menu sub-screens and describes the function. Default settings are in **bold**.

Table 36: Main Setup Menu Sub-screens and Functions

Sub-screen	Description
BIOS Information>	Read only field

Sub-screen	Description
BIOS Information>	BIOS Information, FSP information, PSE information, Board information, Processor information, PCH information, Package information and ME Firmware information
System Language>	Choose the system default language: [**English**]
Platform Information>	Read only field Module Information Product name, Revision, Serial # ,MAC address, Boot counter, and CPLD rev
System Date>	Displays the system date [Week day mm/dd/yyyy]
System Time>	Displays the system time [hh:mm:ss]

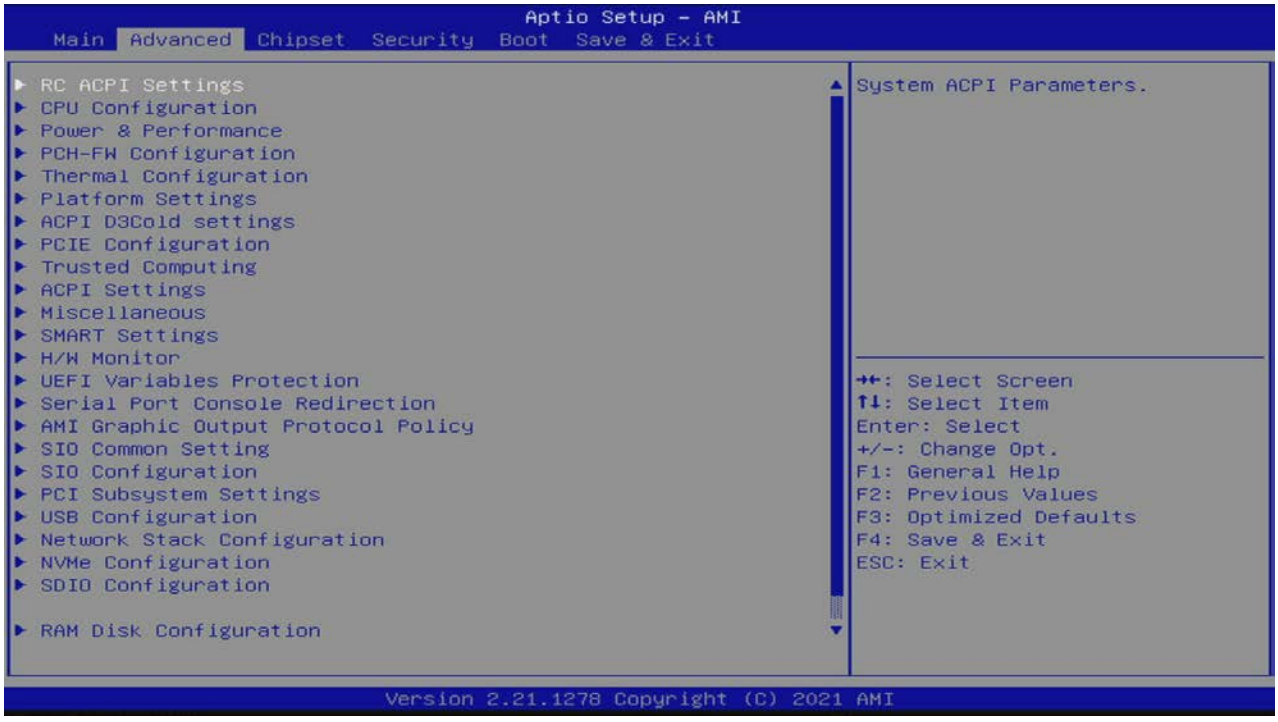
9.5. Advanced Setup Menu

The Advanced Setup menu provides sub-screens and second level sub-screens with functions, for advanced configuration and Kontron specific configurations.

NOTICE

Setting items, on this screen, to incorrect values may cause system malfunctions.

Figure 17: Advanced Setup Menu



The following table shows the Advanced sub-screen and describes the function. Default settings are in **bold**.

Table 37: Advanced Setup Menu Sub-screens and Functions

Sub-screen	Next Level Sub-screens / Description	
RC ACPI Settings>	Native PCIE Enable>	Bit - PCIE Native * Control 0.- hot plug 1. - SHPC native Hot plug control 2. - Power management 3. - PCIe Advanced error reporting 4 – PCIe capability structure control 5- Latency Tolerance reporting control [**Enabled**, Disabled]
	Native ASPM>	Enables – OS control Disabled – BIOS controlled ASPM [Auto, Enabled, **Disabled**]
	Wake System from S5 via RTC>	System wake on alarm event. When enabled system will wake on the hr:min:sec::specified [Enabled, **Disabled**]

Sub-screen	Next Level Sub-screens / Description		
RC ACPI Settings>	Low Power S0 Idle Capability>	Determines If ACPI Lower power S0 idle capability (mutually exclusive with Smart Connect). While enabled 8254 timer is disabled for SLP_S0 support. [Enabled, **Disabled**]	
	PCI Delay Optimization>	Experimental ACPI additions for FW latency optimization [Enabled, **Disabled**	
	MSI Enable>	MSI support is disables in FADT [**Enabled**, Disabled]	
Sub-screen	**Next level Sub-Screens / Description**		
CPU Configuration>	Read only field CPU Configuration: Type, ID, Speed, L1 Data Cache, L1 Instruction Cache, L2 Cache, L3 cache, L4 Cache, VMX, SMX/TXT		
	CPU Flex Ratio Override>	CPU flex ration programming [Enabled, **Disabled**]	
	CPU Flex Ratio Setting>	Read only field CPU Flex Ratio setting [**19**]	
	Hardware Prefetcher>	Turns ON/OFF the MLC streamer prefetcher [**Enabled**, Disabled]	
	Adjacent Cache Line Prefetch>	Turns ON/OFF prefetching of adjacent cache lines [**Enabled**, Disabled]	
	Intel (VMX) Virtualization Technology>	When enabled a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology. [**Enabled**, Disabled]	
	Active Processor Cores>	Number of core to enable in each processor package [**ALL**, 1, 2,3]	
	BIST>	Built-In Self-Test (BIST on reset) [Enabled, **Disabled**]	
	AP Threads Idle Manner>	AP threads idle manner for waiting signal to run [HALT loop, **MWAIT loop**, RUN loop]	
	AES>	Advanced Encryption Standard [**Enabled**, Disabled]	
	Machine Check>	Machine Check [**Enabled**, Disabled]	
	Monitor MWait>	Monitor MWait [**Enabled**, Disabled]	
	CPU SMM Enhancement>	SMM use Delay Indication>	Use of SMM_Delayed MSR for MP sync in SMI [**Enabled**, Disabled]
		SMM use Block Indication>	Use of SMM_Blocked MSR for MP sync in SMI [**Enabled**, Disabled]
		SMM use SMM en-US Indication>	Use of SMM_Enable MSR for MP sync in SMI [**Enabled**, Disabled]

Sub-screen	Next Level Sub-screens / Description			
Power and Performance>	CPU Power Management>	Read only field P1 to P3 Fused Max Core Ratio		
		Boot Performance Mode>	Select the performance state that the BIOS will set starting from rest vector. [Max Battery, Max Non-Turbo Performance, **Turbo Performance**]	
		Intel® Speedstep™>	Allows more than two frequency ranges to be support. [**Enabled**, Disabled]	
		Race to Halt>	RTH dynamically increases CPU frequency in order to enter pkg C-State faster to reduce overall power. (RTH controlled through MSR 1FC bit 20) [**Enabled**, Disabled]	
		View/Configure Turbo options>	Read only field Max/Min turbo limits, Package TDP limit, Power Limit 1 & 2, 1 to 4-Core Turbo Ratio	
			Energy Efficient P-State>	When set to 0: disables access to ENERGY_PERFORMANCE_BIAS MSR and CPUID function 6 ECX [3] reads 0 indicating no support for energy efficient policy setting. When set to 1: enables access to ENERGY_PERFORANCE_BIAS MSR 1B0h and CPUID function 6 ECX [3] will read 1 indicating Energy Efficient Policy is supported. [**Enabled**, Disabled]
			Package Power Limits MSR Lock>	Enable: PACKAGE_POWER_LIMIT MSR locked and a reset required to unlock the register. [Enabled, **Disabled**]
			Power Limit 1 Override>	If disabled: BIOS programs the default values for power limit 1 and power limit 1, time window. [Enabled, **Disabled**]
			Power Limit 2 Override>	If disabled: BIOS programs the default values for power limit 2. [**Enabled**, Disabled]
			Power Limit 2>	Power limit 2 in mW When programming BIOS rounds to nearest 1/8W. If value is 0, BIOS programs this value as 1.25 x TDP. For 12.5W, enter 12500. Processor applied control policies such that the package power does not exceed this limit.[**0**]
			1-Core Ratio Limit Override>	Range 0 to 83. Minimum range varies between processors. This 1-Core ration limit must be greater than or equal to 2-Core/3-Core and 4-Core ratio limit. [**19**]

Sub-screen	Next Level Sub-screens / Description			
Power and Performance>	CPU Power Management>	View/Configure Turbo Options>	2-Core Ratio Limit Override>	Range 0 to 83. Minimum range varies between processors. This 2-Core ration limit must be less than or equal to 1-Core ratio limit. [**19**]
			3-Core Ratio Limit Override>	Range 0 to 83. Minimum range varies between processors. This 3-Core ration limit must be less than or equal to 1-Core ratio limit. 19]
			4-Core Ratio Limit Override>	Range 0 to 83. Minimum range varies between processors. This 4-Core ration limit must be less than or equal to 1-Core ratio limit. [**19**]
			Energy Efficient Turbo>	Lowers frequency to increase efficiency. Disable only in overclocking situations where turbo frequency must remain constant. Otherwise, leave enabled. [**Enabled**, Disabled]
		Platform PL1 Enable>	Platform power limit 1 programming. Enable activates the PL1 value to be used by the processor to limit the average power of given time window. [Enabled, **Disabled**]	
		Platform PL2 Enable>	Platform power limit 2 programming. If disabled BIOS programs the default value for platform Power Limit2 [Enabled, **Disabled**]	
		Power Limit 4 Override>	If disabled BIOS will leave the default values for power limit 4. [Enabled, **Disabled**]	
		C-states	CPU power management. Allows CPU to go to c-states when not 100 utilized [**Enabled**, Disabled]	
		Thermal Monitor>	Enable or disable the thermal monitor [**Enabled**, Disabled]	
		Interrupt redirection Mode Selection>	Selects the logical interrupts [**Fixed Priority**, Round Robin, Hash vector, No Change]	
		Timed MWAIT>	Enable or disables the timed MWait support [Enabled, **Disabled**]	
		Custom P-State Table>	Sets the number of customer P-states. At least 2 states must be present. [**0**]	
		Power Limit 3 Settings>	Read only field	
		CPU Lock Configuration>	CFG Lock>	Configure MSR 0xE2[15], CFG lock bit [**Enabled**, Disabled]

Sub-screen	Next Level Sub-screens / Description			
Power and Performance>	CPU Power Management>	CPU Lock Configuration>	Overclocking Lock>	Overclocking lock (Bit 20) in FLEX_Ratio (194) MSR [Enabled, **Disabled**]
	GT- Power Management Control>	RC6 (Render Standby)>	Checks Enable render standby support [**Enabled**, Disabled]	
		Maximum GT Frequency>	Maximum GT frequency limited by user Choose between 200 MHz (RPN) and 400 MHz (RPO). Value beyond the range clipped to supported min/max by SLU [**Default Max Frequency**, 100MHz, 150MHz, 200MHz ,.....1150MHz, 1200MHz]	
		Disable Turbo GT Frequency>	Enable or Disables the Turbo GT frequency, disable is not limited [Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**			
PCH-FW Configuration>	Read Only field Firmware: version, mode, SKU, States 1, Status 2			
	ME State>	Read only field [**Enabled**, Disabled]		
	ME Unconfig. on RTC Clear>	When disables ME will not unconfigured on RTC clear [**Enabled**, Disabled]		
	Extended CSME Measured to TPM-PCR>	Read only field [Enabled, **Disabled**]		
	Core BIOS Done Message>	Enables or disable the core BIOS Done message sent to ME [**Enabled**, Disabled]		
	Firmware Update Configuration>	ME Firmware Image Re-flash>	Enables or disables the ME firmware image RE-flash function [Enabled, **Disabled**]	
		FW Update>	Enables or disables the ME firmware update function [**Enabled**, Disabled]	
	PTT Configuration>	Read only field PTT Capability/State 1/1 TPM device selection [**PTT**]		
	Anti-Rollback SVN Configuration>	Read only field Minimal allowed Anti-Rollback SVN 0 Executing Anti-Rollback SVN 1		
		Automatic Hardware Enforced Anti-rollback SW>	Anti-rollback automatically active once ME FW successfully runs on platform. Firmware with lower ARB-SVN is blocked from execution [Enabled, **Disabled**]	
		Set HW-enforced Anti-Rollback for Current SVN>	Hardware-enforced anti-rollback for current ARB-SVN value. Firmware with lower ARB-SVN is blocked from execution. Value will be restored to disable after command is sent. [Enabled, **Disabled**]	

Sub-screen	Next Level Sub-screens / Description		
PCH-FW Configuration>	OEM Key Revocation configuration>	Automatic OEM Key Revocation>	BIOS automatically sends HECI command to revoke OEM keys. [Enabled, **Disabled**]
		Invoke OEM Key Revocation>	A Heci command will be sent to revoke OEM key. [Enabled, **Disabled**]
Sub-screen	**Next Level Sub-screens / Description**		
Thermal Consideration>	Enable all Thermal Functions>	Enable: for memory thermal management, active trip points, critical trip points. Disable: for manual configuration [**Enabled**, Disabled]	
	CPU Thermal Configuration>	DTS SMM>	Disable: uses EC reported temperature values. Enable: uses DTS SMM mechanism to obtain CPU temperature values. Out of Spec: uses EC reported temp values and DTS SMM used to handle Out of Spec condition [Enabled, **Disabled,** Critical Temp Reporting]
		TCC Active Offset>	TCC active Offset rage [0 to 63] Temperature at which the thermal control circuit must be activated. [**0**]
		TCC Offset Time Window>	For Running Average Temperature Limits (RATL) feature, the offset time range is 5 ms to 448 s. [**Disabled**, 5ms, 10ms ……..384sec, 488sec]
		TCC Offset Clamp Enable>	For Running Average Temperature Limits (RATL) feature, to allow CPU to throttle below P1 [Enabled, **Disabled**]
		TCC Offset Lock Enable>	For Running Average Temperature Limits (RATL) feature, to lock temperature target MSR. [**Enabled**, Disabled]
		Bi-directional PROCHOT#>	When processor thermal sensor trips (either core) PROCHOT# will be driven. When bi-directional enabled external agents drive PROCHOT# to throttle the processor. [**Enabled**, Disabled]
		Disable PROCHOT# Output>	[**Enabled**, Disabled]
		Disable VR Thermal Alert>	[Enabled, **Disabled**]
		PROCHOT Response>	[Enabled, **Disabled**]
		PROHOT Lock>	[Enabled, **Disabled**]
		ACPI T-States>	[Enabled, **Disabled**]
	Platform Thermal Configuration>	Critical Trip Point>	Controls temperature of ACPI Critical Trip Point, at which OS shuts down the system. Note: 119 C is the PLAN of Record (POR) for all Intel mobile processors. [15 C , 23 C, 31 C……..**119 C (POR)**, 127 C, 130 C]
		Critical trip Points>	[**Enabled**, Disabled]
		PCH Temp Read>	[**Enabled**, Disabled]

Sub-screen	Next Level Sub-screens / Description		
Thermal Consideration>	Platform Thermal Configuration>	CPU Energy Read>	[**Enabled**, Disabled]
		CPU Temp Read>	[**Enabled**, Disabled]
		Alert Enable Lock>	Locks all Alert enable settings. [Enabled, **Disabled**]
		CPU Temp>	Fail safe temp that EC uses if OS hangs [**72**]
		CPU Fan Speed>	Fan speed EC uses if OS hangs [**65**]
Sub-screen	**Next Level Sub-screens / Description**		
Platform Settings>	HID Event Filter driver>	Enable or disable the HID event filter driver interface to OS [**Enabled**, Disabled]	
	System Time and Alarm Source>	Selects source of system time and alarm functions [**ACPI Time and Alarm Device**, Legacy RTC]	
	Intel® Trusted Device Setup Boot>	Enable or disable Intel® Trusted Device setup boot on the next boot. [Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**		
ACPI D3Cold Settings>	ACPI D3Cold Support>	[**Enabled**, Disabled]	
	VR Ramp up Delay>	Delay between subsequent VR ramp ups if they are all turned on at the same time [**16**]	
	PCIE Slot 5 Device Power-On-Delay in ms>	Delay between applying core power and deasserting PERST# [**100**]	
	Audio Delay>	Delay after applying power to HD Audio (REALtek) codec device. [**200**]	
	Sensor Hub>	Delay after applying power to sensor hub device [**68**]	
	TouchPad>	Delay after applying power to touchpad device [**68**]	
	TouchPanel>	Delay on PR _ON after applying power to touch panel device [**68**]	
	P-State Capping>	Set _PPC and send ACPI notification [Enabled, **Disabled**]	
	USB Port 1>	USB RTD3 support. Superspeed USB 3.0 exposed as RTD3 capable. Highspeed: USB 2.0 devices exposed as RTD3 capable. Disabled: USB RTD3 support disabled. For Sawtoothpeak USB port1 (below) is Superspeed and port2(top) is highspeed. Check respective board configuration to know about USB port position. [Highspeed, Superspeed, **Disabled**]	

Sub-screen	Next Level Sub-screens / Description		
ACPI D3Cold Settings>	USB Port 2>	USB RTD3 support. Superspeed USB 3.0 exposed as RTD3 capable. Highspeed: USB 2.0 devices exposed as RTD3 capable. Disabled: USB RTD3 support disabled. For Sawtoothpeak USB port1 (below) is Superspeed and port2(top) is highspeed. Check respective board configuration to know about USB port position. [Highspeed, Superspeed, **Disabled**]	
	ZPODD>	Zero power ODD (ZPODD) only for board with SPODD support [Enabled, **Disabled**]	
	WWAN>	Read only field [**D0/L1.2**]	
	SATA Port 0>	Control the SATA port RTD3 functionality [Enabled, **Disabled**]	
	SATA Port 1	Control the SATA port RTD3 functionality [**Enabled**, Disabled]	
	SATA Port 2>	Control the SATA port RTD3 functionality [Enabled, **Disabled**]	
	SATA Port 3>	Control the SATA port RTD3 functionality. [Enabled, **Disabled**]	
	SATA Port 4>	Control the SATA port RTD3 functionality. [Enabled, **Disabled**]	
	SATA Port 5>	Control the SATA port RTD3 functionality. [Enabled, **Disabled**]	
	PCIe Remapped CR1>	PCIe RTD3 setup conflicts with SATA RTD3. Platform specific [Enabled, **Disabled**]	
	PCIe Remapped CR2>	PCIe RTD3 setup conflicts with SATA RTD3. Platform specific [Enabled, **Disabled**]	
	PCIe Remapped CT3>	PCIe RTD3 setup conflicts with SATA RTD3. Platform specific [Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**		
PCIE Configuration>	IMR Configuration>	PCIe IMR>	[Enabled, **Disabled**]
Sub-screen	**Next Level Sub-screens / Description**		
Trusted Computing>	Read only field TPM 2.0 device, Firmware version, Vendor		
	Security Device Support>	BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available. [**Enabled**, Disabled]	
	Active PCR Banks>	Read Only Field [**SHA256**]	
	Available PCR Banks>	Read only field [**SHA-1, SHA256, SHA384, SM3**]	
	SHA-1 PCR Bank>	[Enabled, **Disabled**]	
	SHA256 PCR Bank>	[**Enabled**, Disabled]	

Sub-screen	Next Level Sub-screens / Description		
Trusted Computing>	SHA_384 PCR Bank>	[Enabled, **Disabled**]	
	SM3_256 PCR Bank>	[Enabled, **Disabled**]	
	Pending operation>	Schedule an operating for security device. Note: computer reboots during restart to change the state of security device. [**None**, Clear]	
	Platform Hierarchy>	[**Enabled**, Disabled]	
	Storage Hierarchy>	[**Enabled**, Disabled]	
	Endorsement Hierarchy>	[**Enabled**, Disabled]	
	TPM 2.0 UEFI Spec Version>	TCG_1_2: compatible mode for Win8/Win10 TCG_2: support for TCG2 protocol and event format for Win 10 or later [TCG_1_2, **TCG_2**]	
	Physical presence Spec Version>	OS supports PPI Spec 1.2 or 1.3. Note: Some HCK tests might not support 1.3. [1.2, **1.3**]	
	TPM 2.0 Interface Type>	Read only field [**CRB**]	
	Device Select>	TPM 1.2 restricts support to TPM 1.2. TPM 2.0 restricts support to TPM 2.0. Auto supports both with the default set to TPM 2.0 devices if not found. TPM 1.2 devices will be enumerated. [TPM 1.2, TPM 2.0, **Auto**]	
Sub-screen	**Next Level Sub-screens / Description**		
ACPI Settings>	Enable ACPI Auto Configuration>	[Enabled, **Disabled**]	
	Enable Hibernation>	System ability to hibernate (OS/S4 sleep state) Note: This option may not be effective with some operating systems. [**Enabled**, Disabled]	
	ACPI Sleep State>	Selects the highest ACPI sleep state the system will enter when suspend is pressed. [Suspend Disabled, **S3 (suspend to Ram)**]	
Sub-screen	**Next Level Sub-screens / Description**		
Miscellaneous>	Generic eSPI Decode Ranges>	Generic LPC via eSPI Decode 1>	Enable generic LPC via eSPI decode range [Enabled, **Disabled**]
	Watchdog>	Auto–Reload>	Automatic reload of watchdog timers on timeout [Enabled, **Disabled**]
		Global Lock>	Enable: watchdog registers (except WD-Kick) read only until board is reset- [Enabled, **Disabled**]
		Stage 1 Mode>	Selects action for this watchdog stage [**Disabled**, reset, Delay, WDT Signal only]
	Rest Button Behavior>	Selects reset button behavior [**Chipset Reset**, Power Cycle]	

Sub-screen	Next Level Sub-screens / Description	
Miscellaneous>	I2C Speed>	Speed in KHz (Min. 1 KHz and max. 400 KH). 200 KHz is an appropriate default value. [**200**]
	Onboard I2C Mode>	Selects Multi master or Busclear [**Multimaster**, Busclear]
	Manufacture Mode>	Read only field [Enabled, **Disabled**]
	Lid Switch Mode>	Shows or hides LID switch in ACPI OS. [Enabled, **Disabled**]
	Sleep Button Mode>	Shows or hides sleep button in ACPI OS [Enabled, **Disabled**]
	ACPI Temperature Polling>	Sets mode for temperature polling through OSPM (0: disabled, 1: enabled) [**Enabled**, Disabled]
	TZ00 Temperature Polling Time>	Interval (sec) between two temperature measuring attempts in ACPI thermal zone 00 (Ambient temperature) [**30]**
	Create ACPI AC adapter>	Creates ACPI AC adapter device with virtual battery even in non-battery systems. This helps some device drivers to identify the power status of the system. [**Enabled**, Disabled]
	SMbus Device ACPI Mode>	SM bus device is hidden or visible in OS [Hidden, **Normal**]
	CPLD Device ACPI Mode>	CPLD device is hidden or visible in OS [Hidden, **Normal**]
	SDIO/GPIO Mode	Read only field [H/W strap]
	SDIO Clock Limit	Auto: used the highest clock the controller and card can agree to, otherwise limit controller clock to given value. [Auto, **25 MHz (SDR12)**, 50 MHz (SDR25), 100 MHz (SDR50)
	GPIO Mux0 Select	GPIO MUX0 select help [GPIO4 Enable, **External HAD Reset Enabled**]
	GPIO Mux1 Select	GPIO MUX1 select help [GPIO5+GPIO6 Enabled, **System Fan Enabled**]
	Control SMARC GPIOs in BIOS>	GPIO control in BIOS- If disable GPIO are not touched by BIOS [Enabled, **Disabled**]
	GPIO IRQ#>	Sets IRQ# to trigger by the CPLD on GPIO event. [Enabled, **Disabled**]
	I2C IRQ#>	Sets the IRQ number to trigger by cPLD on I2C event. [Enabled, **Disabled**]
	Local FW Update>	Allows BIOS re-flashing if Relax Security Configuration is set as enabled. Only Valid for one reset cycle! [Enabled, **Disabled**]
	Last System Reset Through>	Read only field [**Power-on reset**]

Sub-screen	Next Level Sub-screens / Description	
Smart Settings>	Smart Self-test>	Runs Smart self-test on all HDDs during Post [Enabled, **Disabled**]
Sub-screen	**Next Level Sub-screens / Description**	
Hardware Monitor>	Read only field H/W Monitor type, CPU and Modules temperature value and runtime and standby voltage	
	CPU Fan>	
	Fan Control>	Sets fan control mode where disable totally stops the fan. [Disabled, Manual**, Auto**]
	Fan Pulse>	Number of pulses the fan produces during one revolution (range 1 - 4) [**2**]
	Fan Trip Point Speed>	Temperature where the fan accelerates. (range 20 to 80 C) [**50**]
	Trip Point Speed>	Fan speed at trip point in %. Minimum value 30. Fan always runs at 100% at TJmax 10 C. [**50**]
	Reference Temperature>	Determines the temperature source used for automatic fan control [**CPU temperature**, Module temperature]
	External Fan>	
	Fan Control>	Sets fan control mode where disable totally stops the fan. [Disabled, Manual**, Auto**]
	Fan Pulse>	Number of .pulses the fan produces during one revolution (range 1- 4) [**2**]
	Fan Trip Point Speed>	Temperature at which the fan accelerates (range 20 to 80 C) [**50**]
	Trip Point Speed>	Fan speed at trip point in %. Minimum value 30. Fan always runs at 100% at TJmax 10 C.[**50**]
	Reference Temperature>	Determines the temperature source used for automatic fan control [CPU temperature, **Module temperature**]
Sub-screen	**Next Level Sub-screens / Description**	
UEFI Variables Protection>	Password Protection of Runtime Variables>	Controls NVRA; runtime variable protection through system admin Password. [**Enabled**, Disabled]
Sub-screen	**Next Level Sub-screens / Description**	
Serial Port Console Redirection>	COM0	
	Console Redirection>	[Enabled, **Disabled**]
	COM1	
	Console Redirection>	[Enabled, **Disabled**]
	COM3(PCI Bus0, Dev30, Func1, Port1) (disabled)	
	Console Redirection (Kontron COM1)	[Enabled, **Disabled**]
	Serial port for out of Band management/Windows emergency Management Services (EMS)	

Sub-screen	Next Level Sub-screens / Description		
Serial Port Console Redirection>	Console Redirection EMS>	[Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**		
AMI Graphics Output Protocol Policy>	Read only field Intel® Graphics Controller / Intel® GOP Driver [18.0.1031]		
	Output Select>	Selects output Interface [eDP1, **DVI1 Active**]	
	BIST Enable>	Starts of stops BIST on the integrated display panel [Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**		
SIO Common Settings>	Lock Legacy Resource>	[Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**		
SIO Configuration>	Active Serial port 0>	Use this Device>	Enable or disable use of this logical device [**Enabled**, Disabled]
		Logical Device Settings Current>	Read only field IO=3F8h; IRQ=4;
		Possible:>	Allows the user to change the device's resource settings. New settings are reflected on the setup page after system restart. [**Use Automatic Settings**, IO=3F8h; IRQ=4; IO=3F8h; IRQ=3,4,5,7,9,10,11,12; IO=2F8h; IRQ=3,4,5,7,9,10,11,12; IO=3E8h, DMA; IRQ=3,4,5,7,9,10,11,12; IO=2E8h; IRQ=3,4,5,7,9,10,11,12]
	Warning! Disabling SIO logical devices may have unwanted side effects. Proceed with caution!		
	Active Parallel Port 1>	Use this Device>	Enable or disable use of this logical device [**Enabled**, Disabled]
		Logical Device Settings Current>	Read only field IO=2F8h; IRQ=3;
		Possible: Use Automatic Settings:>	Allows the user to change the device's resource settings. New settings are reflected on the setup page after system restart. **Use Automatic Settings**, IO=3 IO=2F8h; IRQ=3; IO=378h; IRQ=3,4,5,7,9,10,11,12; IO=2F8h; IRQ=3,4,5,7,9,10,11,12; IO=3E8h, DMA; IRQ=3,4,5,7,9,10,11,12; IO=2E8h; IRQ=3,4,5,7,9,10,11,12]
	Warning! Disabling SIO logical devices may have unwanted side effects. Proceed with caution!		

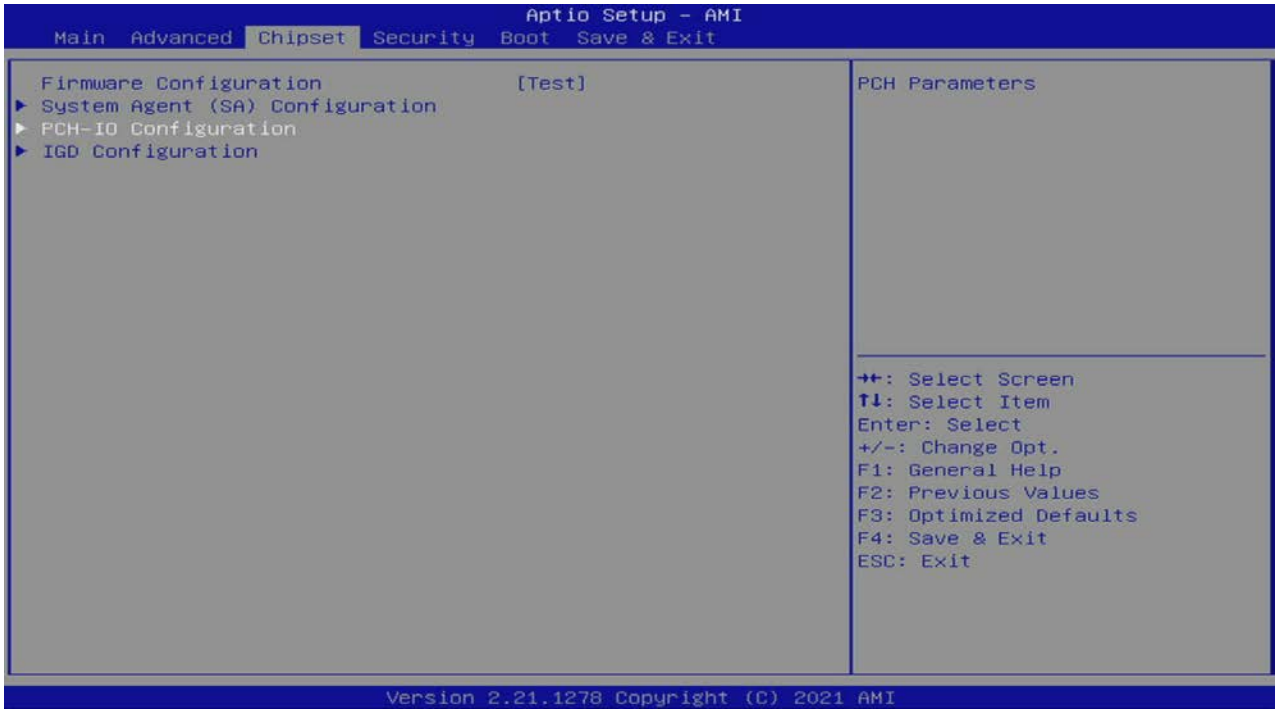
Sub-screen	Next Level Sub-screens / Description	
PCI Sub System Settings>	PCI Settings Common for all Devices:	
	BME DMA Mitigation>	Re-enable Bus Master Attribute disabled during PCI enumeration for PCI Bridge after SMM locked. [Enabled, **Disabled**]
	Change settings of the following PCI devices: Warnings: Changing the PCI device settings may have unwanted side effects. System may hang! Proceed with caution.	
Sub-screen	**Next Level Sub-screens / Description**	
USB Configuration>	Read only field USB module version Controller and devices	
	Legacy Support>	Auto: disable legacy if no USB devices are connected Disable: keeps USB devices available only for EFI applications [**Enabled**, Disabled, Auto]
	XHCI Hand-off>	This is a work around for OSs without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver [**Enabled**, Disabled]
	USB Mass Storage Driver Support>	[**Enabled**, Disabled]
	USB hardware delays and timeouts:	
	USB Transfer Time-outs>	Time out value for control, Bulk and interrupt transfers. [1 sec, 5 sec, 10 sec, **20 sec**]
	Device Reset Time-out>	USB Mass Storage device start unit command time-out [10 sec, **20 sec**, 30 Sec, 40 sec]
	Device Power-Up Delay>	Maximum time device takes before reporting properly to host controller Auto uses default value: 100 ms for a root port, for a Hub port the delay is taken from HUB descriptor. [**AUTO,** Manual]
	Mass Storage devices:	
	Linux File-CD Gadget 0510>	Mass storage device emulation type. Auto enumerates devices according to their media format. Optical drives are emulated as CDROM, drives with no media will be emulated according to a drive type. [**Auto**, Floppy, forces FDD, Hard Disk, CD-Rom]
Sub-screen	**Next Level Sub-screens / Description**	
Network Stake Configurator>	Network Stack>	Enable or disable UEFI network stack. [Enabled, **Disabled**]
Sub-screen	**Next Level Sub-screens / Description**	
NVMe>	Read only field No device found in the system	
Sub-screen	**Next Level Sub-screens / Description**	
SDIO Configuration>	SDIO Access Mode>	Auto: Access SD device in DMA mode if supported else in PIO Mode DMA: access SD device in DMA mode PIO: access SD in PIO mode [**Auto**, ADMA, SDMA, PIO]

Sub-screen	Next Level Sub-screens / Description		
SDIO Configuration>	Mass Storage Devices		
	BUS 0 Dev 1A Fun 0 SOJ58X(63.6GB)>	Mass storage device emulation type. Auto: enumerates devices less than 530 MB as floppies. Forced FDD: forces HDD formatted drive to boot FDD [**Auto**, Floppy, Forced FDD, hard Disk]	
Sub-screen	**Next Level Sub-screens / Description**		
User Password Management>	Admin Password Management>	Read only field [**Not Installed**]	
	Change Admin Password>	New password must be between 8 and 32 Characters include lower and upper case, number and symbol. Note: input old admin password If it was set, then you can change the password to a new one. After the change action you may need to enter the password when you enter UI. Input an empty password can clean old admin password, then no need to input password to enter UI.	
Sub-screen	**Next Level Sub-screens / Description**		
RAM Disk Configuration>	Disk Memory Type>	Specifies type of memory to use from the available memory pool in system to create a disk [**Boot Service Data**, Reserved]	
	Create RAW>	Size Hex>	Valid RAM disk size should be multiples of the RAM disk block size.
		Create & Exit>	Create a new RAM disk with the given starting and ending address
		Discard & Exit>	Discard and exit
	Create from File>	Create a RAM disk from a given file.	
	RAM Disk 0: [0x6D3EA018, 0x6D3EB017]	Select or remove [Enabled, **Disabled**]	
	RAM Disk 1: [0x6D3DD018, 0x6D3DE017]	Select or remove [Enabled, **Disabled**]	
	RAM Disk 2: [0x6D3D9018, 0x6D3DA017]	Select or remove [Enabled, **Disabled**]	
	Remove Selected RAM Disk (s)>	Remove selected RAM disks	

9.6. Chipset

The Chipset Setup menu lists sub-screens and second level sub-screens of the functions supported within the Chipset setup menu.

Figure 18: Chipset Setup Menu



The following table shows sub-screens and describes the function. Default settings are in **bold**.

Table 38: Chipset Setup Menu Sub-screens and Functions

Sub-screen	Next Level Sub-screens / Description				
Firmware Configuration>	Firmware Configuration option. Note Ignore policy update (STR_FW_CONFIG_DEFAULT_VALUE) is to skip policy update and will only work on a platform. [Ignore Policy Update, Production, **Test**]				
Sub-screen	Next Level Sub-screens / Description				
System Agent (SA) Configuration>	VT-d >	Read only field Memory configuration parameters [Supported]			
	Memory Configuration>	Memory Thermal Configuration>	Memory Power and Thermal Throttling>	DDR Power Down and Idle Counter>	BIOS: controls DDR CKE mode and idle timer value. PCODE: manages the mode [PCODE, **BIOS**]
				For LPDDR: DDR Power Down and Idle Counter>	BIOS: controls DDR CKE mode and idle timer value. PCODE: manages the mode [PCODE, **BIOS**]

Sub-screen	Next Level Sub-screens / Description				
System Agent (SA) Configuration>	Memory Configuration>	Memory Thermal Configuration>	Memory Power and Thermal Throttling>	Refresh_2X_ Mode>	0-disabled, **1- IMC Enables 2xRef when Warm or Hot**, 2- IMC Enables 2xref when Hot. [disabled, **1- Enabled for warm or hot**, 2- enabled for hot only]
				LPDDR Thermal Sensor>	When enabled MC uses MR4 to read LPDDR thermal sensors [**Enabled**, Disabled]
				Self Refresh Enable>	[**Enabled**, Disabled]
			Memory Thermal Management>	[Enabled, **Disabled**]	
		Read only field Memory configuration: RC Version, Date rate and Timings. Slot information (populate (size, rank, manufacturer), not populated) Memory ratio and clocking/overclocking			
		MCR ULT Safe Config.>	MCR ULT safe Configuration for P0 [Enabled, **Disabled**]		
		Safe Mode Support>	Used for changes/WAs that may affect a stable MRC [Enabled, **Disabled**]		
		Maximum Memory Frequency>	Maximum frequency (MHz) must divide by 133 or 100 according to RefCLK. In GEAR2 must divide by 2666or 200. Lowest GEAR2 speed is 2133. [**Auto**, 1067, 1200….. 4200, 4267		
		Max TOULD>	Dynamic assignment adjusts TOLUD automatically based on the largest MMIO length of installed graphics controller. [**Dynamic**, 1GB, 1,25GB, 1.5GB, 1.75GB, 2GB, 2.25GB, 2.5GB]		
		SA GV>	System Agent Geyserville. Can disable, fix to a specific point, or enable frequency switching. [Disable, Fixed Low, Fixed Mid, Fixed High, **Enabled**]		
		Enables RH Prevention>	Actively prevent row hammer [**Enabled**, Disabled]		
		Row Hammer Solution>	Type of method to prevent row hammer [**2x refresh**]		
		Power Down Mode>	CKE power Down Mode Control [**Auto**, No Power Down, APD, PPD-DLLoff]		
		Memory Scrambler>	Enables/ disable memory scrambler support [**Enabled**, Disabled]		

Sub-screen	Next Level Sub-screens / Description		
System Agent (SA) Configuration>	Memory Configuration>	Force ColdReset>	Force Coldreset or Choose MrcColdBoot mode, when Coldboot is required during MRC execution- If ME 5 MB is present, Force Coldreset is required! [Enabled, **Disabled**]
		IN-Band ECC>	[**Enabled**, Disabled]
		IN-Band ECC Operation Mode>	0: functional mode protects requests on the address range 1: makes all requests non protected and ignores range checks, 2: makes all requests protected and ignores range check [0, 1, **2**]
		In-Band ECC Error Injection>	By enabling the error injection enabling feature, the user acknowledges the security risks. Enabling error injection allows attackers who have access to the host operating system to inject IBECC errors that can cause unintended memory corruption and enable the leak of security data in the BIOS stolen memory regions. [Enabled, **Disabled**]
		Memory Remap>	Memory remap above 4 GB [**Enabled**, Disabled]
		Fast Boot>	Fast path through the MRC [**Enabled**, Disabled]
		Train On Warm Boot>	Training on warm boot [Enabled, **Disabled**]
		BDAT Memory Test Type>	Read Only field [**Rank margin Tool Rank**]
	Graphics Configuration>	Skip Scanning of External Gfx Card>	Enabled- will not scan for external Gfx card on PEG and PCH PCIe ports [Enabled, **Disabled**]
		Primary Display>	Select the IGFX/PEG/PCI graphics device which is the primary display or select HG for hybrid Gfx. [**Auto**, IGFX, PEG, PCI]
		External Graphics Cards Primary Display Configuration>	Primary PCIE> : Select: Auto/PCIE1 to PCIe7 of D28: F0 to F7, PCIE8 to PCIE15 of D29: F0 to FF7, PCIE16 to PCIe19 of D27: F0 to F3, Graphics device should be primary PCIE [**Auto**, PCIE1, PCIe2, …….. PCIE18, PCIE19]
		Internal Graphics>	Keep IGFX enabled based on the Setup options [**Auto**, Disabled, Enabled]
		GTT Size>	Selects GTT size [2MB, 4MB, **8MB**]
		Aperture Size>	Select the aperture size. Note: above 4GB MMIO BIOS assignments is automatically enabled when selecting 2048 MB aperture. To use this feature please disable CSM support. [128MB, **256MB**, 512MB, 1024MB]

Sub-screen	Next Level Sub-screens / Description		
System Agent (SA) Configuration>	Graphics Configuration>	DVMT Pre-allocated>	Selects the pre-allocated (fixed) graphics memory size used by the internal graphics device [32M, 64M, 96M 128M, 160M, 4M, 8M, 12M , 16M, 20M, 24M, 28M, 32M/F7, 36M, 40M, 44M, 48M, 52M, 56M , **60M**]
		DVMT Total Gfx Mem>	Selects the total graphics memory size used by the internal graphics device [128M, **256M**, Max]
		PM Support>	[**Enabled**, Disabled]
		PAVP Enable>	[**Enabled**, Disabled]
	VT-d>	[**Enabled**, Disabled]	
	X2APCI Opt Out>	X2APCI Opt Out bit [**Enabled**, Disabled]	
	DMA Control Guarantee>	DMA Control Guarantee bit [Enabled, **Disabled**]	
	IGD VTD Enable>	[**Enabled**, Disabled]	
	IPU VTD Enable>	[Enabled, **Disabled**]	
	IOP-VTD Enable>	[**Enabled**, Disabled]	
	CPU Crash Log (Device 10)>	[Enabled, **Disabled**]	
	CRID Support>	SA CRID and TCSS CRID control for Intel SIPP [Enabled, **Disabled**]	
	Above 4 GB MMIO BIOS Assignment>	Enables/ disables above 4 GB memory mapped Io BIOS assignment. This is enabled automatically when aperture size is set to 2048 MB. [**Enabled**, Disabled]	

Sub-screen	Next level Sub-Screens / Description		
PCH-IO Configuration>	PCI Express Configuration>	DMI Link ASPM Control>	Control of Active State power management of the DMI [Disable, L0s, L1, L0sL1, **Auto**]
		Peer Memory Write Enable>	[Enabled, **Disabled**]
		Compliance Test Mode>	[Enabled, **Disabled**]
		PCH PCI Express Clock Gating>	PCH PCI express clock gating (power management) for each root port. [Platform-POR, Enabled, **Disabled**]
		PCIe Function Swap>	Disabled prevents PCIe root port function swap. If any function other than 0^{th} is enabled, 0^{th} will become visible. [**Enabled**, Disabled]

Sub-screen	Next Level Sub-screens / Description			
PCH-IO Configuration>	PCI Express Configuration>	PCIe EQ Settings>	PCIe EQ Override>	Choose own PCIe EQ setting. Only use when you have a thorough understanding of the equalization process. [Enabled, **Disabled**]
		PCIE Express Root Port [1 to 4]>	PCIe Express Root Port [#]>	Control the PCIe Express Root Port [**Enabled**, Disabled]
			Connection Type>	Read only field [**Slot**]
			ASPM>	Sets ASPM level: Force L0: Forces all links to L0s state Auto: BIOS auto configure Disable: Disables ASPM [**Disable**, L0s, L1, L0sL1, Auto]
			L1 Sub-states>	PCI express L1 sub-state settings: [**Disabled**, l1.1, l1.1 &L1.2]
			ACS>	Access Control Service extended capabilities [**Enabled**, Disabled]
			PTM>	Precision Time Measurement Enabled, **Disabled**]
			DPC>	Downstream Port Containment [**Enabled**, Disabled]
			EDPC>	Extensions for Downstream Port Containment [**Enabled**, Disabled]
			URR>	Unsupported Request Reporting [Enabled, **Disabled**]
			FER>	Fatal error reporting [Enabled, **Disabled**]
			NFER>	Non- Fatal error reporting [Enabled, **Disabled**]
			CER>	PCIe Correctable error reporting [Enabled, **Disabled**]
			SEFE>	Root PCIe System error on fatal error [Enabled**, Disabled**]
			SENFE>	PCIe System error on non-fatal error [Enabled, **Disabled**]
			SECE>	Root PCIe System error on correctable error [Enabled, **Disabled**]
			PME SCI>	PCIe PME SCI [**Enabled**, Disabled]

Sub-screen	Next Level Sub-screens / Description				
PCH-IO Configuration>	PCI Express Configuration>	PCIE Express Root Port [1 to 4]>	Hot Plug>	PCIe hotplug [Enabled, **Disabled**]	
			Advance Error Reporting>	[**Enabled**, Disabled]	
			PCIE Speed>	Configure PCIe Speed [**Auto**, Gen1, Gen2, Gen3]	
			Transmitter Half Swing>	[Enabled, **Disabled**]	
			Detect Timeout>	Time (msec) the reference code waits for link to exit detect state for enabled ports before assuming no device and potentially disabling the port. [**0**]	
			Extra Bus Reserved>	Extra bus reserved (0-7) for bridges behind this root bridge [**0**]	
			Reserved Memory>	Range (1-20 MB) for this root port. [1**0**]	
			Reserved I/O>	Reserved IO Range (4K, 8K, 12K, 16K, 20K) for this root bridge. [**4**]	
			PCH PCIe LTR Configuration		
			LTR>	PCIe latency reporting [**Enabled**, Disabled]	
			Snoop Latency Override>	Snoop latency override for PCH PCIe: Disabled- disable override Manual- Manually enter override values Auto- maintain default BIOS flow [Disabled, Manual**, Auto**]	
			Non Snoop Latency Override>	Non Snoop latency override for PCH PCIe: Disabled- disable override Manual- Manually enter override values Auto- maintain default BIOS flow [Disabled, Manual, **Auto**]	
			Force LTR Override>	Force LTR override for PCH PCIe: Enabled: LTR override values are forced and LTR messages from the device ignored Disabled: LTR override values are not forced [Enabled, **Disabled**]	
			LTR Lock>	PCIe LTR configuration lock [Enabled, **Disabled**]	
			Extra Options>	Detect Non-Compliance Device>	When enabled device will take more post time [Enabled, **Disabled**]

Sub-screen	Next Level Sub-screens / Description				
PCH-IO Configuration>	PCI Express Configuration>	PCIE Express Root Port [1 to 4]>	Extra Options>	Prefetch Memory>	Prefetchable memory range for this root bridge [**10**]
				Reserved Memory Alignment>	Range (0 to 31 bits) [**1**]
				Prefetchable Memory Alignment>	Range (0 to 31 bits) [**1**]
		PCI Clock>	Clock0 Assignment>	Platform-POR = clock assigned to PCIe port or LAN according to module layout Enable = keep clock even if unused Disable = disable clock [Platform-POR, **Enabled**, Disabled]	
			ClkReq for Clock0>	Platform-POR = CLKREQ signal assigned to CLKSRC according to module layout Disable = disable clock [Platform-POR, **Disabled**]	

Sub-screen	Next Level Sub-screens / Description			
PCH-IO Configuration>	SATA Configuration>	SATA Controllers>	Enable/disable SATA device [**Enabled,** Disabled]	
		SATA Mode Selection>	Determines how the SATA controllers(s) operate [**AHCI**]	
		SATA Ports Multiplier>	[Enabled, **Disabled**]	
		SATA Test Mode>	Test mode enable disable (loop back) [Enabled, **Disabled**]	
		Software Feature Mask Configuration>	HDD Unlock>	Enabled: Indicates HDD password unlock in OS is enabled [**Enabled,** Disabled]
			LED Locate>	Enabled: Indicates LED/SGPIO hardware is attached and ping to locate feature is enabled on OS [**Enabled,** Disabled]
		Aggressive LPM Support>	Enable PCH to aggressively enter link power state [**Enabled**, Disabled]	
		Serial ATA Port 0>	Read only field **Empty**	
		Software Preserve>	Read only Field **Unknown**	
		Port [#]>	Enable or disable the SATA port [0 or 1] [**Enabled**, Disabled]	
		Hot Plug>	Designates port as hot pluggable [Enabled, **Disabled**]	

Sub-screen	Next Level Sub-screens / Description		
PCH-IO Configuration>	SATA Configuration>	Configure as eSATA>	Read only Field **Hot Plug Supported**
		External>	Marks port as External [Enabled, **Disabled**]
		SPIN Up Device>	Enables staggered spin up on boot (on drives with option enabled spin up only). Otherwise all drives spin up at boot [Enabled, **Disabled**]
		SATA Device Type>	Identified the drive type connected to SATA port [**Hard Disk Drive**, Solid State drive]
		Topology>	Identify the SATA topology [**Unknown**, ISATA, Direct Connect, Flex, M2]
		SATA Port 0 DevSLP>	For DevSLP both hard drive and SATA port need to support DevSLP function otherwise, unexpected behavior might happen. Check module design before enabling. [Enabled, **Disabled**]
		SATA Port 0 RXPolarity>	Enable/disable SATA Port 0 RXPolarity. Disable is default- check module design before enabling. [Enabled, **Disabled**]
		DITO Configuration>	[Enabled, **Disabled**]
		DITO Value>	Read Only port [**625**]
		DM value>	Read Only port [**15**]
Sub-screen	**Next Level Sub-screens / Description**		
PCH-IO Configuration>	USB Configuration>	XHCI Compliance Mode>	Disabled: Default Enable: for Compliance mode testing [Enabled, **Disabled**]
		XDCI Support>	Read only field [Enabled, **Disabled**]
		USB2 PHY Sus Well Power Gating>	Select Enable for Sus Well PG for USB2 PHT. This option has no effect on PCH-H. [**Enabled**, Disabled]
		USB3 Link Speed Selection>	Selects USB3 link speed [**GEN 1**, GEN2]
		USB PDO Programming>	Select if Port Disable Override (PDO) used [**Enabled**, Disabled]
		USB Overcurrent>	Select Disable for pin-based debug. If Pin-based debug enabled and USB overcurrent is not disabled, USB DbC does not work. [**Enabled**, Disabled]

Sub-screen	Next Level Sub-screens / Description			
PCH-IO Configuration>	USB Configuration>	USB Overcurrent Lock>	Select Enable if USB Overcurrent functionality is used. Enabling make xHCI controller consume overcurrent mapping data [**Enabled**, Disabled]	
		USB Port Disable Override>	Enable or disable the corresponding USB port from reporting a device connection to the controller [**Disabled**, Select Per-Pin]]	
		USB Device/HOST Mode Override>	Enable or disable the corresponding USB 2.0 and USB 3.0 port device mode [**Disabled**, Select Per-Pin]	
Sub-screen	**Next Level Sub-screens / Description**			
PCH-IO Configuration>	Security Configuration>	RTC Memory Lock>	Enable Locks bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM [**Enabled,** Disabled]	
		BIOS Lock>	PCH BIOS Lock enable feature. Enable to ensure SMM protection of Flash. [**Enabled,** Disabled]	
Sub-screen	**Next Level Sub-screens / Description**			
PCH-IO Configuration>	HD Audio Configuration>	HD Audio>	Controls detection of the HD-audio device: Enables or disable: HDA unconditionally [**Enabled,** Disabled]	
		Audio DSP>	Enables or disables the Audio DSP. [Enabled, **Disabled**]	
		HD Audio Advanced Configuration>	iDisplay Audio Disconnect>	Disconnects the SDI2 signal to hide/disable iDisplay audio Codec [Enabled, **Disabled**]
			Codec Sx Wake Capability>	Capability to detect wake initiated by a codec in Sx (e.g. Modem codec) [Enabled, **Disabled**]
			PME Enable>	Enables PME wake of HD audio controller during post [Enabled, **Disabled**]
			Statically Switchable VBCLK Clock Frequency Config.	
			HD Audio Link Frequency>	Selects HD Audio Link frequency. Applicable only if HAD codec supports selected frequency [6 MHz, 12 MHz, **24 MHz**]
			iDisplay Audio Link Frequency>	Selects iDisplay Link frequency [48 MHz, **96 MHz**]
			iDisplay Audio Link T-Mode>	Indicates whether SDI is operating in 1T, 2T (CNL) or 2T, 4T, 8T mode (ICL) [2T Mode, 4T Mode, **8T Mode**, 16T Mode]

Sub-screen	Next Level Sub-screens / Description			
PCH/IO Configuration>	Serial IO Configuration>	SPI2 Controller>	The SPI2 depend on the thermal subsystem in PCI mode. Otherwise, SPI2 will not appear in the OS. SPI2 will be disabled if PSE SPIO or PWM or TGPIO is enabled. [Enabled, **Disabled**]	
		UART1 Controller (COMe UART0>	If device is function 0, PSF disabling is skipped. PSF default remains and device PCI CFG space will be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1,2,3 UART0 and UART1, SPIO, 1 UART2 and I2C4,5 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 [Disabled, **Enabled**, Communication port (COM)]	
		Serial IO UART1 Settings>	Hardware Flow Control>	Enable: configures two additional GPIO pads for use as RTS/CTS signals for UART [Enabled, **Disabled**]
			DMA Enable>	Enable: UART OS driver uses DMA when possible Disable: OS driver enforces PIO mode [**Enabled**, Disabled]
Sub-screen	**Next Level Sub-Screens / Description**			
PCH/IO Configuration>	SCS Configuration>	eMMC 5.1 Controller>	[**Enabled,** Disabled]	
		eMMC 5.1 HS400 Mode>	[**Enabled,** Disabled]	
		Enable HS400 Software Tuning>	Software tuning should improve eMMC HS400 stability at the expense of boot time. [Enabled, **Disabled**]	
		Driver strength>	Sets I/O driver strength [33 Ohm, **40 Ohm**, 50 Ohm]	
		SD Card 3.0 Controller>	Enables disable SCS SDHC 3.0 controller [Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-Screens / Description**			
PCH-IO Configuration>	PSE Configuration>	PSE Controller>	Enables/disable Programmable Service Engine (PSE) device [**Enabled,** Disabled]	

Sub-screen	Next Level Sub-screens / Description		
PCH-IO Configuration>	PSE Configuration>	PSE IP ownership and GPIO Mux Assignment Configuration	
		I2SC7>	If I2C7 is not set to host owned, all PSE CAN and QEP devices could not be set to host owned too due to sharing same function. I2C7 cannot assign host own if UCSI ACPI device enabled [**None**, PSE owned with pin muxed, Host owned with pin muxed]
		SPI0>	SPI0 has pin conflict with PWM pin 3, TGPIO pin 10-13 and 39, serial SPI2. If it is greyed out, check the previous options. The same pin cannot be assigned to multiple IP. IF SPI0 is not set to host owned, SPI1-3 could not be set to host owned too due to sharing same function. [**None**, PSE owned with pin muxed, Host owned with pin muxed]
		SPI1>	To assign this device to host owned enable PSE SPI0 to host owned because SPI0 is the function 0 of the device: SPI0 has pin conflict with PWM, TGPIO10-14, 39, serial IO SPI2, SPI1 has pin conflict with PWM, TGPIO32-35-. SPI2 has pin conflict with serial IO SPI0 SPI3 has pin conflict with serial IO SPi1. If it is greyed out, check the previous options [**None**, PSE owned with pin muxed]
		CAN0>	I2C7 to host owned because I2C7 is a function of 0 of this device: CAN0 has pin conflict with I2S0 and TGPIO 16-17 CAN1 has pin conflict with I2S0 and TGPIO14.15. If it is greyed out, check the previous options. The same pin cannot be assigned to multiple IP. [**None**, PSE owned with pin muxed]
		CAN1>	[**None**, PSE owned with pin muxed]
		PSE Interrupt Assignment Configuration	
		SPI0>	Checked = interrupt set to SB mode. Default unchecked is MSI mode. [Enabled, **Disabled**]
		SPI1>	Checked = interrupt set to SB mode. Default unchecked is MSI mode. [Enabled, **Disabled**]
		CAN0>	Checked = interrupt set to SB mode. Default unchecked is MSI mode. [Enabled, **Disabled**]
		CAN1>	Checked = interrupt set to SB mode. Default unchecked is MSI mode. [Enabled, **Disabled**]

Sub-screen	Next Level Sub-screens / Description		
PCH-IO Configuration>	TSN GBE Configuration>	PCH TSN LAN Measurement>	Enable/disable TSN LAN. This will mux RGMII2 PPS and RGMII AUXTS. Disable PSE I2C7 to enable this option. [Enabled, **Disabled**]
		PCH TSN GBE Multi-Vc>	Enable or disable TSN Multi Virtual Channels. [Enabled, **Disabled**]
		PCH TSN GBE SGMII Support>	Enable or disable SGMII mode for PCH TSN GBE. Port in SGMII mode with the same PLL common lane must use the same link speed. SATA or UFS needs to be disables if TSN port is using the same PLL common lane. Make sure IFWI has the proper straps set for SGMII. Make sure FLEX IO lane assignment is not NONE. [**Enabled,** Disabled]
		PCH TSN link Speed>	PSE TSN GBE 0 link speed configuration. [RefClk 38.4MHz 2.5Gbps, **RefClk 38.4MHz 1Gbps**]
		Flex IO Lane Assignment>	Read only field [**Lane 8**]
		PSE TSN GBE 0 Multi-VC>	Enable or disable TSN Multi Virtual Channels. TSN GBE must be host owned. [Enabled, **Disabled**]
		PSE TSN GBE 0 SGMII Support>	Enable or disable Modphy support for SGMII mode with the same PLL common lane must use the same link speed. UFS needs to be disables as this post uses the same PLL common lanes. Make sure IFWI has the proper straps set for SGMII. Make sure FLEX IO lane assignment is not NONE. [**Enabled,** Disabled]
		PSE TSN GBE 0 Link Speed>	PSE TSN GBE 0 link speed configuration. [RefClk 38.4MHz 2.5Gbps, **RefClk 38.4MHz 1Gbps**]
		Flex IO Lane Assignment>	Read only field [**Lane 7**]

Sub-screen	Next Level Sub-screens / Description	
PCH/IO Configuration>	PCH Master Clock Gating Control>	[Disabled, **Default**]
	PCH Master Power Gating Control>	[**Disabled**, Default]
	State After G3>	Specifies state to go to when power is re-applied after a power failure (G3 State) [**S0 state**, S5 State]
	Port 80h Redirection>	Controls where the port 80h cycles are sent [**LPC Bus**, PCIE Bus]
	Enhance Port 80h LPC Decoding>	Support the word/dwor decoding of port 80h behind LPC [**Enabled,** Disabled]

Sub-screen	Next Level Sub-screens / Description	
PCH/IO Configuration>	Legacy IO Low Latency>	Set the enable low latency of legacy IO. Some systems require lower IO latency irrespective of power. This is a tradeoff between power and IO latency. [Enabled, **Disabled**]
	PCH Energy Reporting>	Enable energy Report. MUST set as ENABLED. This is only for test purposes. [**Enabled,** Disabled]
	LPM S0i2.0>	Enables or disables the S0ix sub-states. This setting is for test purpose. S0ix sub-states should be enables for production. [**Enabled,** Disabled]
	LPM S0i2.1>	
	LPM S0i2.2>	
	LPM S0i3.0>	
	LPM S0i3.1>	
	LPM S0i3.2>	
	LPM S0i3.3>	
	LPM S0i3.4>	
	IEH Mode>	Enable or Bypass IEH Mode [**Bypass**, Enabled]
	Enable TCO Timer>	Enables or disables TCO timer. When disables, it disables PCH ACPI timer, stops TCO timer and ACPI WDAT table will not be published. [Enabled, **Disabled**]
	PCIe PLL SSC>	PCIe PLL SSC percentage Auto: Keep HW default, no BIOS override (range 0.0% to 2.0%) [**Auto**, 0.0%, 0.1%, 0.2%, …. 2.0%, Disabled]
	Flash Protection Range Register>	Enables the flash protection range registers (FRPP) [Enabled, **Disabled**]
	LGMR>	64 KB memory block for LGMR (LPC Memory Range Decode) [**Enabled,** Disabled]
	Extended BIOS Range Decode>	Enable: redirects memory cycles falling in a specific area to SPI flash controller. [Enabled, **Disabled**]

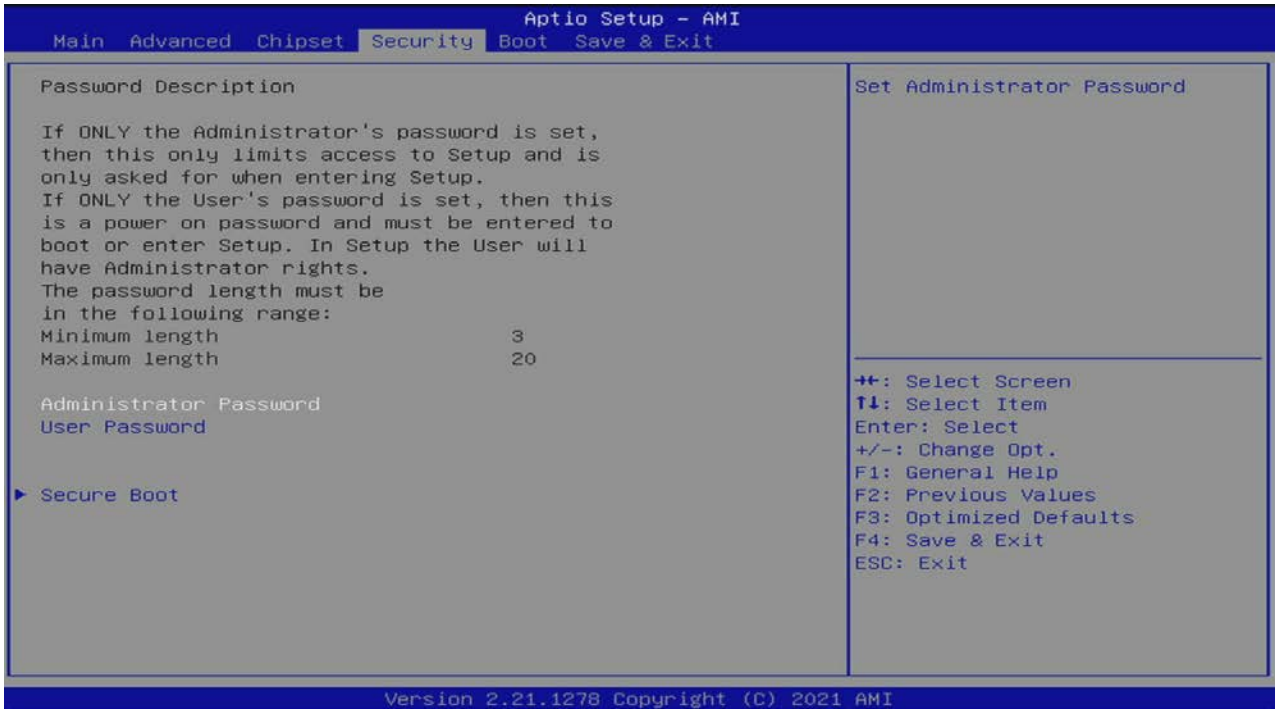
Sub-Screen	Next level Sub-screens / Description	
IGD configuration>	eDP Port Configuration	
	eDP Port>	Help: eDP [**Enabled,** Disabled]
	Integrated eDP to LVDS Bridge>	Help: integrated eDP to LVDS bridge [Disabled, **Auto**]
	LFP Resolution>	Selects the LFP used by internal graphics device: [**Auto,** VGA 640x480 1x18 WVGA 800x480 1x18, SVGA 800x600 1x18 XGA 1024x768 1x18, XGA 1024x768 1x24 WXGA 1280x768 1x24, WXGA 1280x800 1x18 WXVGA 1366x768 1x24, WSVGA 1024x600 1x18

Sub-screen	Next Level Sub-screens / Description	
IGD configuration>	LFP Resolution> (continued)	WSVGA 1024x600 1x24, …..WXGA+ 1440x900 2x18 WXGA+ 1440x900 2x24, SXGA 1280x1024 2x18, SXGA 1280x1024 2x24, WSXGA+ 1680x1050 2x18 WSXGA+ 1680x1050 2x24, UXGA 1600x1200 2x18 UXGA 1600x1200 2x24, WUXGA 1920x1200 2x18 WUXGA 1920x1200 2x24, FHD 1920x1080 2x18 FHD 1920x1080 2x24, Custom PAID]
	Panel Channel Mode>	For internal LVDS EDID 1.3 detection, select the panel channel Mode. Auto chooses the setting will be determined during the next start and the switch will be set to 'Single' or 'Dual' [**Auto,** Single, Dual]
	Backlight Control>	Backlight control setting. [None/External, **PWM**, PWM Inverted, I2C, I2C Inverted]
	PWM Frequency>	Set LCD backlight PWM frequency. [**200 Hz**, 400 Hz, 1 kHz, 2 kHz, 4 kHz, 8 kHz, 20 kHz, 40 kHz]
	Backlight Value>	Set LCD Backlight brightness (1-255). [**255**]
	LVDS Clock Center Spreading>	Select the LVDS Clock frequency center spreading depth [**No Spreading**, 0.5%, 1.0%, 1.5%, 2.0%, 2.5%]

9.7. Security Setup Menu

The Security Setup menu provides information about the passwords and functions for specifying the security settings. The passwords are case-sensitive.

Figure 19. Security Setup Menu



The following table shows the Security sub-screens and describes the function. Default settings are in **bold**.

Table 39: Security Setup Menu Sub-screens and Functions

Sub-screen	Next Level Sub-screens / Description		
Setup Administrator Password>	Sets administrator password		
User Password>	Sets user password		
Secure Boot>	Secure Boot>	Enable to activate. Platform key (PK) is enrolled and the system is in user mode. Mode change requires platform reset. [Enabled, **Disabled**]	
	Secure Boot Mode>	Custom: secure boot policy variable can be configured by a physically present user without full authentication. [Standard, **Custom**]	
	Restore Factor Keys>	Install factor defaults [Yes, No]	
	Reset to Set Up Mode>		
	Vendor keys	Read only field [valid]	
	Key Management>	Factory Key Provision>	Restore factory default after platform rest and while system is in setup mode [Enabled, **Disabled**]

Sub-screen	Next Level Sub-screens / Description		
Secure Boot>	Key Management>	Restore Factor Keys>	Restore factor defaults [Yes, No]
		Reset to Set Up Mode>	
		Export Secure Boot Variables>	
		Enroll Efi Image>	Allows image to run in secure boot mode. Enroll SHA256 Hash certificate of a PE image into authorized signature Database (db). Select a file system from the available options.
		Device Guard Ready	
		Remove UEFI CA from DB>	
		Restore DB Defaults>	Restore DB variable to factor defaults [Yes, No]
		*S*ecure Boot Variable	/ Size / Keys / Key source
		Platform Key>	Enroll factory defaults or load certificate from a file: 1. Public key certificate: a. EFI_Signature_List b. EFI_cert_X509 (DER) c. EFI_CERT_RSA2048 (bin) d. EFI_CERT_SHAXXX 2. Authenticated UEFI variable 3. EFI PE/COFF Image(SHA256) Key Source: Factory, External, Mixed
		Key Exchange Keys>	
		Authentication Signature>	
		Forbidden Signatures>	
		Authorize Timestamps>	
		OSRecovery Signatures >	

If only the administrator's password is set, then only access to the setup is limited and is requested when entering the setup. If the user's password is set, then the password is a power on password and must be entered to boot or enter setup. In the setup the user has restricted rights.

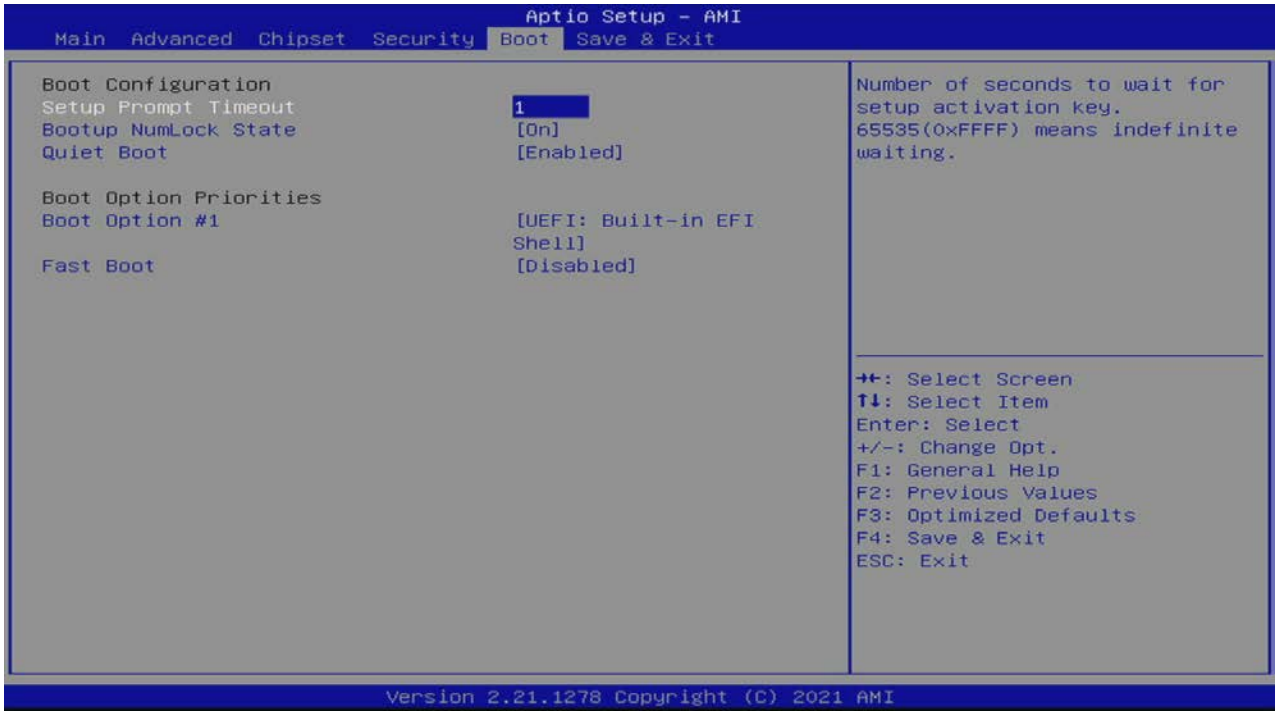
9.7.1. Remember the Password

It is highly recommended to keep a record of all passwords in a safe place. Forgotten passwords result in the user being locked out of the system. If the system cannot be booted because the User Password or the Supervisor Password are not known, contact Kontron Support for further assistance.

9.8. Boot Setup Menu

The Boot Setup menu lists dynamically generated boot device priority order.

Figure 20: Boot Setup Menu



The following table shows the Boot Setup sub-screens and describes the function. Default settings are in **bold**.

Table 40: Boot Setup Menu Sub-screens and Functions

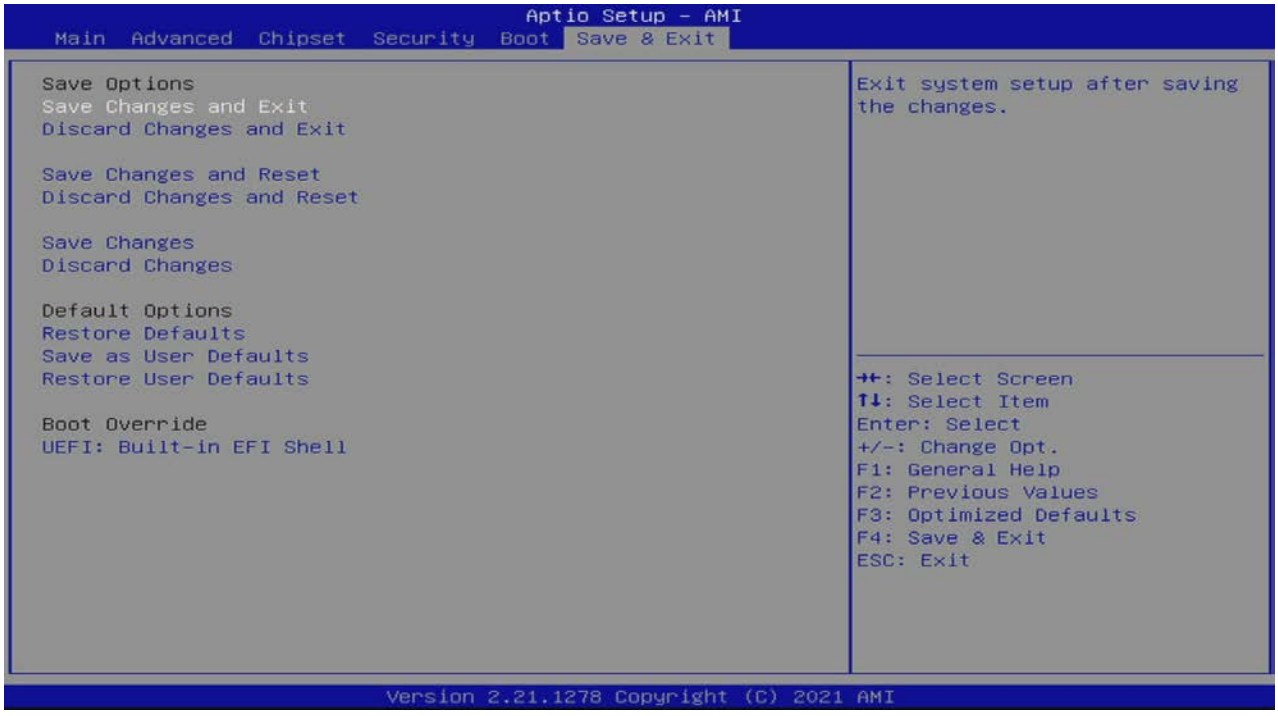
Sub-screen	Description
Setup Prompt Timeout>	Number of seconds that the firmware waits for setup activation key The value 65535(0xFFFF) means an indefinite wait. [**1**]
Bootup NumLock State>	Selects keyboard NumLock state. [**ON**, OFF]
Quiet Boot>	[**Enabled**, Disabled)
Boot Option Priorities:	
Boot Option #1>	Sets the system boot order [UEFI: Built in EFI Shell, Disabled]
Fast Boot>	Enables or disables Boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS Boot option. [Enabled, **Disabled**]

Only boot from module BIOS or carrier BIOS supported, no other boot options supported:

9.9. Save and Exit Setup Menu

The Save and Exit Setup menu provides functions for handling changes made to the uEFI BIOS settings and exiting the Setup program.

Figure 21: Save and Exit Setup Menu



If system cannot boot or work properly due to incorrect setting, activating the Force Recovery jumper will load the default setting of BIOS upon power cycle. Please check with your SMARC Carrier System provider for more information. Once safely booted with default setting, you may deactivate the Force Recovery jumper to save new changes on BIOS setting.

The following table shows the Save and Exit sub-screens and describes the function.

Table 41: Save and Exit Setup Menu Sub-screens and Functions

Sub-screen	Description
Save Options:	
Save Changes and Exit >	Exits system set up after saving changes [Yes, No]
Discard Changes and Exit>	Exits system setup without saving changes [Yes, No]
Save Changes and Reset>	Resets system after saving changes [Yes, No]
Discard Changes and Reset>	Resets system setup without saving changes [Yes, No]
Save Changes>	Saves changes made so far for any setup options [Yes, No]
Discard Changes>	Discards changes made so far for any setup options [Yes, No]
Default Options:	
Restore Defaults>	Restores/loads standard default values for all setup options [Yes, No]

Sub-screen	Description
Save as User Defaults>	Saves changes done so far as user defaults [Yes, No]
Restore User Defaults>	Restores user defaults to all setup options [Yes, No]
Boot Override:	
UEFI: Built in EFI Shell>	[Yes, No]

10/ Technical Support

For technical support contact Kontron's Support department:

- E-mail: support@kontron.com
- Phone: +49-821-4086-888

Make sure you have the following information available when you call:

- Product ID Number (PN)
- Serial Number (SN)
- Module's revision
- Operating System and Kernel/Build version
- Software modifications
- Addition connected hardware/full description of hardware set up

The serial number can be found on the product's type label.

10.1. Returning Defective Merchandise

All equipment returned to Kontron must have a Return of Material Authorization (RMA) number assigned exclusively by Kontron. Kontron cannot be held responsible for any loss or damage caused to the equipment received without an RMA number. The buyer accepts responsibility for all freight charges for the return of goods to Kontron's designated facility. Kontron will pay the return freight charges back to the buyer's location in the event that the equipment is repaired or replaced within the stipulated warranty period. Follow these steps before returning any product to Kontron.

1. Visit the RMA Information website:

   http://www.kontron.com/support-and-services/support/rma-information

2. Download the RMA Request sheet for **Kontron Europe GmbH –Deggendorg** and fill out the form. Take care to include a short detailed description of the observed problem or failure and to include the product identification Information (Name of product, Product number and Serial number). If a delivery includes more than one product, fill out the above information in the RMA Request form for each product.

3. Send the completed RMA-Request form to the fax or email address given on the RMA Request sheet and Kontron will provide an RMA-Number.

4. The goods for repair must be packed properly for shipping, considering shock and ESD protection.

Goods returned to Kontron in non-proper packaging will be considered as customer caused faults and cannot be accepted as warranty repairs.

5. Include the RMA-Number with the shipping paperwork and send the product to the delivery address provided in the RMA form or received from Kontron RMA Support.

11/ Warranty

Kontron defines product warranty in accordance with regional warranty definitions. Claims are at Kontron's discretion and limited to the defect being of a material nature. To find out more about the warranty conditions and the defined warranty period for your region, following the steps below:

1. Visit Kontron's Term and Conditions webpage.

   http://www.kontron.com/terms-and-conditions

2. Click on your region's General Terms and Conditions of Sale.

11.1. Limitation/Exemption from Warranty Obligation

In general, Kontron shall not be required to honor the warranty, even during the warranty period, and shall be exempted from the statutory accident liability obligations in the event of damage caused to the product due to failure to observe the following:

- Safety instructions within this user guide
- Warning labels on the product and warning symbols within this user guide
- Information and hints within this user guide

Additionally, alterations or modifications to the product that are not explicitly approved by Kontron, described in this user guide, or received from Kontron Support as a special handling instruction will void your warranty.

Within the warranty period, the product should only be opened by Kontron. Removing the protection label and opening the product within the warranty period exempts the product from the statutory warranty obligation.

Due to their limited service life, parts that by their nature are subject to a particularly high degree of wear (wearing parts) are excluded from the warranty beyond that provided by law.

List of Acronyms

Table 42: List of Acronyms

ACPI	Advanced Configuration and Power Interface
COM	Computer-on-Module
CPLD	Complex Programmable Logic Device
ECC	Error Checking and Correction
DDI	Digital Display Interface
DDR4	Double Data Rate Gen 4
DIMM	Dual In-line Memory Module
DP	Display Port
eDP	embedded Display Port
EDID	Extended Display Identification Data
GbE	Gigabit Ethernet
GOIO	General Purpose IO
GPU	Graphics Processing Unit
HD/HDD	Hard Disk /Drive
HDMI	High Definition Multimedia Interface
HSIO	High Speed IO
HWM	Hardware Monitor
I2C	Inter-Integrated Circuit
IOL	IPMI-Over-LAN
IOT	Internet of Things
IPMI	Intelligent Platform Management Interface
LPS	Limited Power Source
LVDS	Low Voltage Differential Signaling
MAC	Media Access Control (Ethernet layer)
MCP	Multi Chip Package
MEI	Management Engine Interface
NA	Not Applicable
PCH	Platform Controller Hub
PCIe	PCI-Express®
PECI	Platform Environment Control Interface
PEG	PCI-Express® Graphics
PHY	Physical Ethernet Layer
PICMG®	PCI Industrial Computer Manufacturers Group
PSE	Programmable Service Engine
RTC	Real Time Clock
SATA	Serial Advanced Technology Attachment
SELV	Safety Extra Low Voltage
SIO	Super IO
SMBus	System Management Bus
SOC	System on Chip
SOL	Serial Over LAN
SPI	Serial Peripheral Interface
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface

About Kontron

Kontron is a global leader in IoT/Embedded Computing Technology (ECT). Kontron offers individual solutions in the areas of Internet of Things (IoT) and Industry 4.0 through a combined portfolio of hardware, software and services. With its standard and customized products based on highly reliable state-of-the-art technologies, Kontron provides secure and innovative applications for a wide variety of industries. As a result, customers benefit from accelerated time-to-market, lower total cost of ownership, extended product lifecycles and the best fully integrated applications.

For more information, please visit: **www.kontron.com**

Global Headquarters

Kontron Europe GmbH

Gutenbergstr. 2
85737 Ismaning, Germany
Tel.: + 49 821 4086-0
Fax: + 49 821 4086-111
info@kontron.com