TQMxCU1-HPCM
User's Manual

TQMxCU1-HPCM UM 0104
27.08.2025

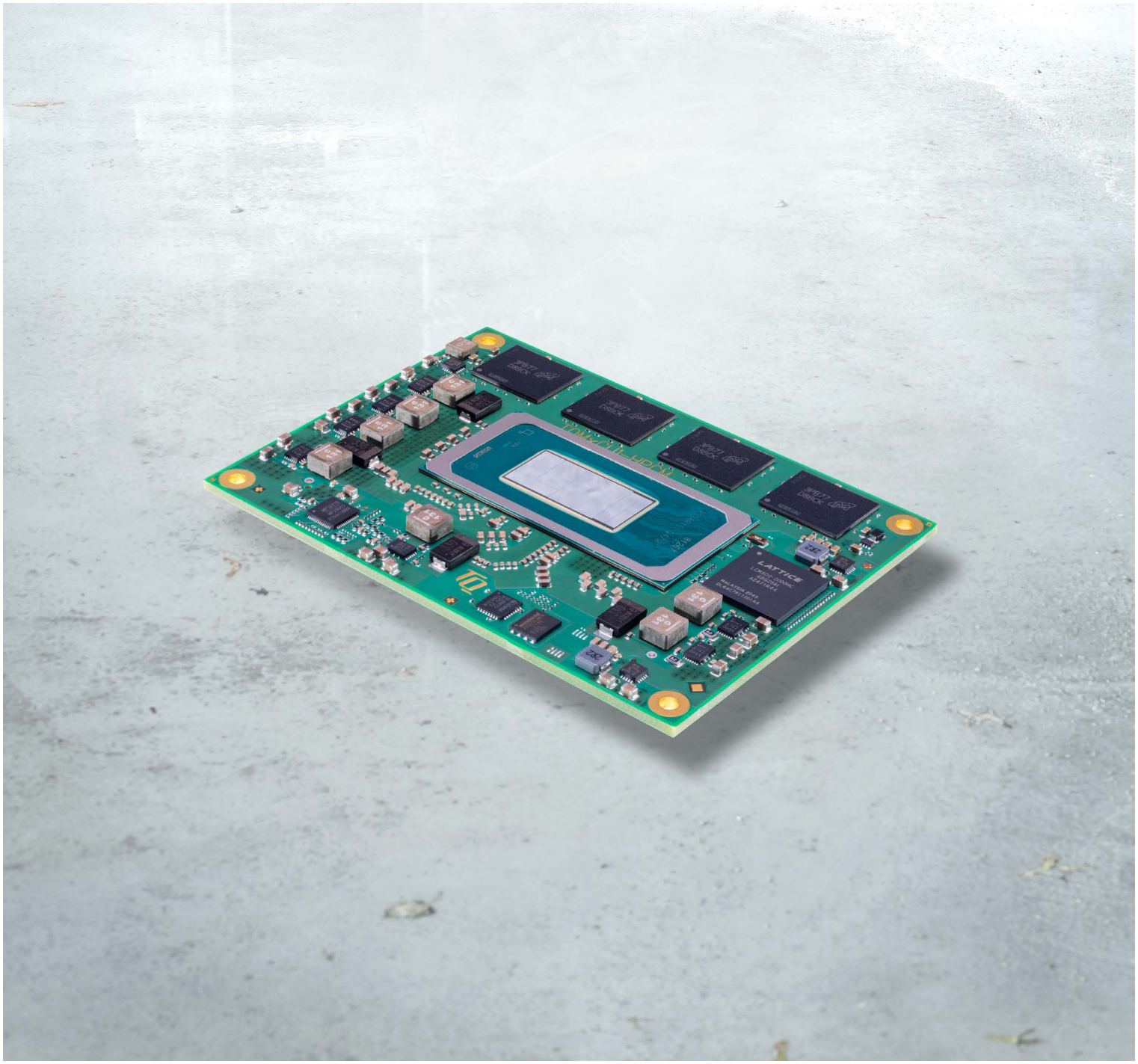

TABLE OF CONTENTS

TABLE DIRECTORY

FIGURE DIRECTORY

REVISION HISTORY

Rev.	Date	Name	Pos.	Modification
0100	15.10.2024	KG		First release
0101	21.11.2024	HM	All	General update
0102	12.12.2024	KG	Table 3, Table 4 3.5.9 Table 18	Power consumption updated Updated Removed
0103	04.06.2025	KG	3.5.2	USB4 description added
0104	27.08.2025	KG	3.5.2.1	USB Type-C configuration update

1. ABOUT THIS MANUAL

1.1 Copyright and License Expenses

This User's Manual may not be copied, reproduced, translated, changed or distributed, completely or partially in electronic, machine readable, or in any other form without the written consent of TQ-Systems GmbH.

The drivers and utilities for the components used as well as the BIOS are subject to copyrights of the respective manufacturers. The licence conditions of the respective manufacturer are to be adhered to.

BIOS-licence expenses are paid by TQ-Systems GmbH and are included in the price.

Licence expenses for the operating system and applications are not taken into consideration and have to be calculated/declared separately.

1.2 Registered Trademarks

TQ-Systems GmbH aims to adhere to copyrights of all graphics and texts used in all publications, and strives to use original or license-free graphics and texts.

All brand names and trademarks mentioned in this User's Manual, including those protected by a third party, unless specified otherwise in writing, are subjected to the specifications of the current copyright laws and the proprietary laws of the present registered proprietor without any limitation. One should conclude that brand and trademarks are rightly protected by a third party.

1.3 Disclaimer

TQ-Systems GmbH does not guarantee that the information in this User's Manual is up-to-date, correct, complete or of good quality. Nor does TQ-Systems GmbH assume guarantee for further usage of the information. Liability claims against TQ-Systems GmbH, referring to material or non-material related damages caused, due to usage or non-usage of the information given in this User's Manual, or due to usage of erroneous or incomplete information, are exempted, as long as there is no proven intentional or negligent fault of TQ-Systems GmbH.

TQ-Systems GmbH explicitly reserves the rights to change or add to the contents of this User's Manual or parts of it without special notification.

1.4 Intended Use

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

You understand and agree that your use of TQ products or devices as a component in your applications are solely at your own risk. To minimize the risks associated with your products, devices and applications, you should take appropriate operational and design related protective measures.

You are solely responsible for complying with all legal, regulatory, safety and security requirements relating to your products. You are responsible for ensuring that your systems (and any TQ hardware or software components incorporated into your systems or products) comply with all applicable requirements. Unless otherwise explicitly stated in our product related documentation, TQ devices are not designed with fault tolerance capabilities or features and therefore cannot be considered as being designed, manufactured or otherwise set up to be compliant for any implementation or resale as a device in high risk applications. All application and safety information in this document (including application descriptions, suggested safety precautions, recommended TQ products or any other materials) is for reference only. Only trained personnel in a suitable work area are permitted to handle and operate TQ products and devices. Please follow the general IT security guidelines applicable to the country or location in which you intend to use the equipment.

1.5 Imprint

TQ-Systems GmbH
Gut Delling, Mühlstraße 2
D-82229 Seefeld

Tel: +49 8153 9308–0
Fax: +49 8153 9308–4223
E-Mail: Info@TQ-Group
Web: www.tq-group.com

1.6 Service and Support

Please visit our website TQ-Group for latest product documentation, drivers, utilities and technical support.
For direct technical support, you can contact our FAE team by email: TQ-Support.
Our FAE team can also support you with additional information like 3D-STEP files and confidential information, which is not provided on our public website.
For service or RMA, please contact our Service or your sales representative.

1.7 Tips on Safety

Improper or incorrect handling of the product can substantially reduce its life span.

1.8 Symbols and Typographic Conventions

Table 1: Terms and Conventions

Symbol	Meaning
	This symbol represents the handling of electrostatic-sensitive modules and / or components. These components are often damaged / destroyed by the transmission of a voltage higher than about 50 V. A human body usually only experiences electrostatic discharges above approximately 3,000 V.
	This symbol indicates the possible use of voltages higher than 24 V. Please note the relevant statutory regulations in this regard. Non-compliance with these regulations can lead to serious damage to your health and cause damage / destruction of the component.
	This symbol indicates a possible source of danger. Acting against the procedure described can lead to possible damage to your health and / or cause damage / destruction of the material used.
	This symbol represents important details or aspects for working with TQ-products.
`Command`	A font with fixed-width is used to denote commands, contents, file names, or menu items.

1.9 Handling and ESD Tips

General handling of your TQ-products

	The TQ product may only be used and serviced by certified personnel who have read the information and safety instructions in this document and all related rules and regulations. Generally, do not touch the TQ product while it is operating. This is especially important when turning on, changing jumper settings, or connecting other devices without first ensuring that the system's power supply has been turned off. Violating this guideline can result in damage to or destruction of the TQMxCU1-HPCM and endanger your health. Improper handling of your TQ product will void the warranty.

Proper ESD handling

	The electronic components of your TQ-product are sensitive to electrostatic discharge (ESD). Always wear antistatic clothing, use ESD-safe tools, packing materials etc., and operate your TQ-product in an ESD-safe environment. Especially when you switch modules on, change jumper settings, or connect other devices.

1.10 Naming of Signals

A hash mark (#) at the end of the signal name indicates a low-active signal.

Example: RESET#

If a signal can switch between two functions and if this is noted in the name of the signal, the low-active function is marked with a hash mark and shown at the end.

Example: C / D#

If a signal has multiple functions, the individual functions are separated by slashes when they are important for the wiring.

The identification of the individual functions follows the above conventions.

Example: WE2# / OE#

1.11 Further Applicable Documents / Presumed Knowledge

- **Specifications and manual of the modules used:**
  These documents describe the service, functionality and special characteristics of the module used.
- **Specifications of the components used:**
  The manufacturer's specifications of the components used are to be taken note of.
  They contain, if applicable, additional information that has to be taken note of for safe and reliable operation.
  These documents are stored at TQ-Systems GmbH.
- **Chip errata:**
  It is the user's responsibility to make sure all errata published by the manufacturer of each component are taken note of.
  The manufacturer's advice should be adhered to.
- **Software behaviour:**
  No warranty can be given, nor responsibility taken for any unexpected software behaviour due to deficient components.
- **General expertise:**
  Expertise in electrical engineering / computer engineering is required for the installation and the use of the device.

Implementation information for the carrier board design is provided in the COM-HPC® Carrier Design Guide (3), maintained by the PICMG®. This Carrier Design Guide includes a very good guideline to design a COM-HPC® Mini carrier board.

It includes detailed information with schematics and detailed layout guidelines.

Please refer to the official PICMG® documentation for additional information (2), (4).

COM-HPC® Mini I/O voltages.
The COM-HPC® Mini redefines a number of I/O voltage rails from 3.3 V to 1.8 V, reflecting current chipset and SOC trends. Low-speed, single-ended signals, that are directly attached to the chipset and SOC are redefined on the COM-HPC® Mini to operate at 1.8 V.

2. INTRODUCTION

Based on the internationally established PICMG® standard COM-HPC® Mini (COM-HPC® Module Base Specification Rev. 1.2), the TQMxCU1-HPCM enables the development of powerful and economical x86-based systems. The user has access to all essential CPU interfaces via the COM-HPC® Mini-compliant pin-out connector. This means that all functions of the Intel® Core™ Ultra processor (H-series and U-series) can be used. Direct access to all interfaces gives the user the freedom to use the CPU's functions in the way that best suits their application.

The compact and robust design, as well as the option of conformal coating, extend the range of applications to include harsh industrial, transportation and aviation environments. Due to the very low power consumption and the optional extended temperature range, it is also possible to realize outdoor applications in an easy and reliable way.

2.1 Overview

The following key functions are implemented on the TQMxCU1-HPCM:

Processor:

Intel® Core™ Ultra processor (H-series 28 W) with up to 16 processor cores

- Intel® Core™ Ultra 7 Processor 165H (6P+8E+2LP, up to 5.0 GHz / 128 EU / 24 MB / 28 W)
- Intel® Core™ Ultra 7 Processor 155H (6P+8E+2LP, up to 4.8 GHz / 128 EU / 24 MB / 28 W)
- Intel® Core™ Ultra 5 Processor 135H (4P+8E+2LP, up to 4.6 GHz / 128 EU / 18 MB / 28 W)
- Intel® Core™ Ultra 5 Processor 125H (4P+8E+2LP, up to 4.5 GHz / 112 EU / 18 MB / 28 W)

Intel® Core™ Ultra processor (U-series 15 W) with up to 12 processor cores

- Intel® Core™ Ultra 7 Processor 165U (2P+8E+2LP, up to 4.9 GHz / 64 EU / 12 MB / 15 W)
- Intel® Core™ Ultra 7 Processor 155U (2P+8E+2LP, up to 4.8 GHz / 64 EU / 12 MB / 15 W)
- Intel® Core™ Ultra 5 Processor 135U (2P+8E+2LP, up to 4.4 GHz / 64 EU / 12 MB / 15 W)
- Intel® Core™ Ultra 5 Processor 125U (2P+8E+2LP, up to 4.3 GHz / 64 EU / 12 MB / 15 W)

Memory:

- Up to 64 Gbyte LPDDR5x max. 7467 MT/s SDRAM dual channel, soldered down, with IBECC option
- EEPROM: 32 Kbit (24AA32) (optional)

Graphics:

- 2 × Digital Display Interface / DP++ with up to 8K; with support for Multi-Stream Transport (MST)
- 1 × Embedded Digital Display Interface (eDP)

Peripheral interfaces:

- 2 × NBASE-T Ethernet with 2.5 Gigabit (Intel® i226)
- 4 × USB 3.2 Gen 2 (up to 10 Gb/s) with USB 3.0 compatibility
- 2 × USB4 Support, pins shared with Digital Display Interface
- 8 × USB 2.0
- 4 × PCI Express group low Gen4, up to 16 Gb/s, 4 (×1), 2 (×2), or 1 (×4)
- 4 × PCI Express group low Gen4, up to 16 Gb/s, 4 (×1), 2 (×2), or 1 (×4)
- 4 × PCI Express group high Gen4, up to 16 Gb/s, 1 (×1), 1 (×2), or 1 (×4)
- 4 × PCI Express group high Gen4, up to 16 Gb/s, 1 (×1), 1 (×2), or 1 (×4)
- 1 × Intel® HD audio (HDA)
- 3 × I^2C
- 1 × SMBus
- 1 × eSPI bus for external I/O devices
- 1 × SPI for external UEFI BIOS flash
- 1 × SPI general-purpose interface
- 2 × Serial port, 4-wire (Rx/Tx/RTS/CTS)
- 12 × GPIO through TQ-flexiCFG

Security components:

- Internal firmware TPM (fTPM) controller or discrete TPM with SLB9672 TPM 2.0 controller

Others:

- TQMx86 board controller with watchdog and TQ-flexiCFG
- Temperature monitor and fan control

Power supply voltage:

- Wide input: 8.0 V to 20 V
- 3 V Battery for RTC

Environment:

- Operating standard temperature: 0 °C to +60 °C
- Storage temperature: –40 °C to +85 °C
- Relative humidity (operation): 10 % to 90 % (non-condensing)
- Relative humidity (storage): 5 % to 95 % (non-condensing)

Form factor / dimensions:

- COM-HPC® Mini, 95 mm × 70 mm

2.2 Compliance

The TQMxCU1-HPCM complies with PICMG® standard COM-HPC® Mini (COM-HPC® Module Base Specification Rev. 1.2).

2.3 Versions

The TQMxCU1-HPCM is available in several standard configurations.

Table 2: TQMxCU1-HPCM Module configurations and features (preferred standard versions)

Feature	TQMxCU1-HPCM-AB	TQMxCU1-HPCM-AD	TQMxCU1-HPCM-AF	TQMxCU1-HPCM-AH
Intel® CPU	Intel® Core™ Ultra 7 155H	Intel® Core™ Ultra 5 125H	Intel® Core™ Ultra 7 155U	Intel® Core™ Ultra 5 125U
vPro	No	No	No	No
CPU TDP	28 W	28 W	15 W	15 W
Heat spreader	TQMxCU1-HPCM-HSP-AA	TQMxCU1-HPCM-HSP-AA	TQMxCU1-HPCM-HSP-AA	TQMxCU1-HPCM-HSP-AA
Heatsink incl. fan	TQMxCU1-HPCM-KK-AA	TQMxCU1-HPCM-KK-AA	TQMxCU1-HPCM-KK-AA	TQMxCU1-HPCM-KK-AA
LPDDR5x	16 / 32 / 64 Gbyte	16 / 32 / 64 Gbyte	16 / 32 / 64 Gbyte	16 / 32 / 64 Gbyte
CPU Use Condition	Embedded	Embedded	Embedded	Embedded
Independent displays	3	3	3	3
eDP	1	1	1	1
DP or HDMI *1)	Up to 2	Up to 2	Up to 2	Up to 2
USB4 *1)	Up to 2	Up to 2	Up to 2	Up to 2
USB 3.2 host	4	4	4	4
USB 2.0 host	8	8	8	8
PCI Express lanes	16	16	15 *2)	15 *2)
NBASE-T	2	2	2	2
eSPI	1	1	1	1
SPI (BIOS Flash)	1	1	1	1
GSPI	1	1	1	1
TPM 2.0 (chip)	SLB9672	SLB9672	SLB9672	SLB9672
I²C	3	3	3	3
SMbus	1	1	1	1
HDA	1	1	1	1
UART	2	2	2	2
GPIO	12	12	12	12
I/O voltage	1.8 V	1.8 V	1.8 V	1.8 V

*1) On the Super Speed lane configuration either USB4 #0 or DDI #1 can be used.

*2) The Intel® Core™ Ultra processor U-series only support 15 × PCI Express lanes. Lane 03 is not supported.

Please visit TQ-Group (tab “Ordering Information”) for a full list of standard versions.
Other configurations are available on request. Hardware and software configuration on request:

- Customized BIOS
- Customized High-Speed-Lane configuration (PCIe, USB4 / DDI…)
- Extended specification for use conditions (standard: “embedded” vs. “industrial 24/7”)

2.4 Accessories

- **TQMxCU1-HPCM-HSP-AA**
  Aluminium heat spreader for TQMxCU1-HPCM, according to COM-HPC® Mini specification.
- **TQMxCU1-HPCM-HSP-AB**
  Aluminium heat spreader with copper inlay for TQMxCU1-HPCM, according to COM-HPC® Mini specification.
- **Evaluation platform (Carrier board) MB-COMHPCM-1**
  Mainboard for COM-HPC® Mini, with the following interfaces:
  - 1 × DP up to 4k
  - 1 × eDP or LVDS
  - 1 × USB4 on USB-C or 1 × DP
  - 4 × USB 3.2 USB-A (2 × 5 Gbit/s and 2 × 10 Gbit/s)
  - 1 × USB 2.0 internal
  - 2 × 2.5 Gigabit Ethernet
  - 3 × M.2 Socket Key E PCI Express ×1 (e.g. for Wi-Fi/BT)
  - 2 × M.2 Socket Key M PCI Express ×4 (SSD)
  - 1 × PCI Express ×16 connector with ×4 PCI Express configuration
  - 2 × Serial Port RS232
  - 1 × High Definition Audio (Line In, MIC In, HP Out)
  - 1 × CAN interface
  - Fan header

  Note: Supported features depend on module configuration.
  Configuration/feature set will differ between variants (e.g. USB4 vs. second DP)
- **Debug module**
  POST debug card for TQMxCU1-HPCM, see 3.6.3. The debug card is not a standard accessory.

3. FUNCTION

3.1 Block Diagram

The following figure shows the TQMxCU1-HPCM block diagram.

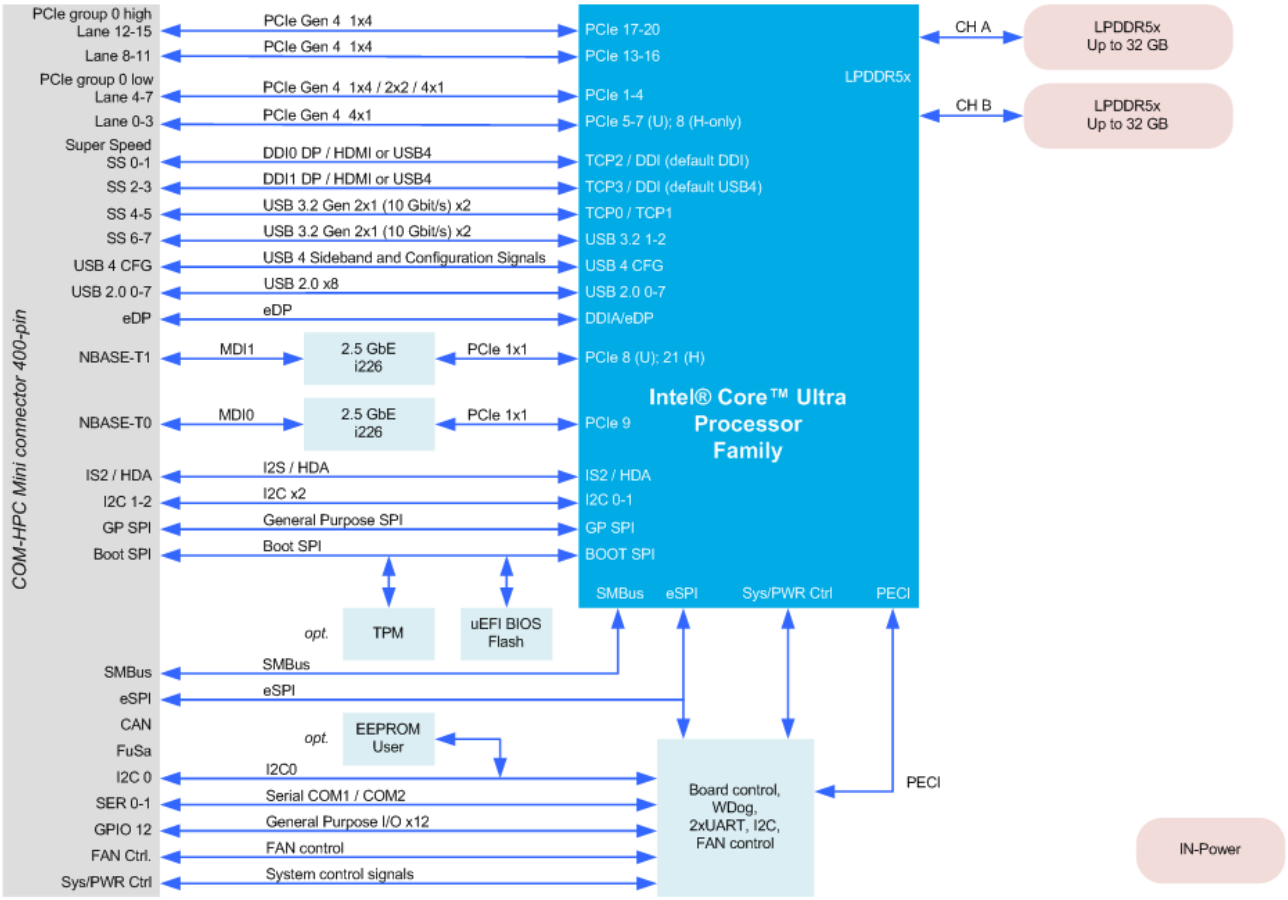

Figure 1: TQMxCU1-HPCM Block Diagram

3.2 Electrical Characteristics

3.2.1 Supply Voltage

The TQMxCU1-HPCM supports a wide-range voltage input from 8.0 V to 20 V.
The following supply voltages are specified at the COM-HPC® Mini connector:

- Wide input: 8.0 V to 20 V
- VCC_RTC: 2.0 V to 3.3 V

The input voltages shall rise from 10 % to 90 % of nominal within 0.1 msec to 20 msec (0.1 msec ≤ Rise Time ≤ 20 msec).
The increase of each DC output voltage has to be smooth and continuous from 10 % to 90 % of its final set point within the regulation range.

3.2.2 Power Consumption

The power consumption values below show the TQMxCU1-HPCM voltage and power specifications.
The values were measured with two power supplies, one for the TQMxCU1-HPCM and the other one for the MB-COMHPCM-1 carrier board.
The power consumption of each TQMxCU1-HPCM version was measured running Windows® 10, 64-bit and an LPDDR5x configuration (32 Gbyte). All measurements were done at +25 °C and an input voltage of +12 V.
The power consumption of the TQMxCU1-HPCM depends on the application, the mode of operation and the operating system.
The power consumption was measured under the following test conditions:

- **Suspend mode:**
  The system is in S5/S4 state, Ethernet ports are disconnected.
- **Windows® 10, 64-bit, idle state:**
  Desktop idle state, Ethernet ports are disconnected.
- **Windows® 10, 64-bit, maximum workload (cTDP down mode enabled):**
  These values show the maximum cTDP down power consumption using the Intel® stress test tool to stress the processor and graphics engine.
- **Windows® 10, 64-bit, maximum workload (cTDP nominal configuration):**
  These values show the maximum worst-case power consumption using the Intel® stress test tool to stress the processor and graphics engine.
- **Windows® 10, 64-bit, maximum workload (cTDP up mode enabled):**
  These values show the maximum cTDP up power consumption using the Intel® stress test tool to stress the processor and graphics engine.
- **Windows® 10, 64-bit, maximum workload (turbo mode first seconds)**
  These values show the maximum worst-case power consumption using the Intel® stress test tool to stress the processor and graphics engine.
  This value was measured only for a short time (<28 sec) when the processor is in turbo mode.
  This value should be used for designing the power supply for the TQMxCU1-HPCM module.

The S3 mode (Suspend to Ram) is not yet supported by the current Intel Windows® and Linux Ubuntu (64-bit) drivers.
Please contact TQ-Support for further information about the S3 software support.

The following table shows the TQMxCU1-HPCM power consumption with different CPUs.
The power consumption in the S5/S4 state is approximately 700 mW.

Table 3: TQMxCU1-HPCM Power Consumption Turbo Mode ON

CPU	Mode				
	Win10, 64-bit idle	Win10, 64-bit cTDP down 20 W max. load	Win10, 64-bit cTDP nominal 28 W max. load	Win10, 64-bit cTDP up max. load	Win10, 64-bit max load (Turbo mode)
Intel® Core™ Ultra H-series 28 W	4.5 W	25 W	34 W	–	87 W
CPU	Win10, 64-bit idle	Win10, 64-bit cTDP down 12 W max. load	Win10, 64-bit cTDP nominal 15 W max. load	Win10, 64-bit cTDP up 28 W max. load	Win10, 64-bit max load (Turbo mode)
Intel® Core™ Ultra U-series 15 W	4.5 W	16 W	19 W	33 W	67 W

Table 4: TQMxCU1-HPCM Power Consumption Turbo Mode OFF

CPU	Mode				
	Win10, 64-bit idle	Win10, 64-bit cTDP down 20 W max. load	Win10, 64-bit cTDP nominal 28 W max. load	Win10, 64-bit cTDP up max. load	Win10, 64-bit max load (Turbo mode)
Intel® Core™ Ultra H-series 28 W	4.5 W	25 W	34 W	–	–
CPU	Win10, 64-bit idle	Win10, 64-bit cTDP down 12 W max. load	Win10, 64-bit cTDP nominal 15 W max. load	Win10, 64-bit cTDP up 28 W max. load	Win10, 64-bit max load (Turbo mode)
Intel® Core™ Ultra U-series 15 W	4.5 W	16 W	19 W	33 W	–

Attention: Power requirement	
	The power supplies on the carrier board for the TQMxCU1-HPCM must be designed with sufficient reserves. The carrier board should be able to provide at least twice the maximum TQMxCU1-HPCM workload power. The TQMxCU1-HPCM supports multiple low-power states. The power supply of the carrier board must be stable, even with no load. Carrier power supply recommendation: Intel® Core™ Ultra processor H-series 28 W max. load Turbo ON Power Consumption = 87 W Carrier power design = 120 W Intel® Core™ Ultra processor H-series 28 W max. load Turbo OFF Power Consumption = 34 W Carrier power design = 70 W Intel® Core™ Ultra processor U-series 15 W max. load Turbo ON Power Consumption = 67 W Carrier power design = 100 W Intel® Core™ Ultra processor U-series 15 W max. load Turbo OFF Power Consumption = 33 W Carrier power design = 70 W

3.2.3 Real Time Clock Power Consumption

The RTC (VCC_RTC) current consumption is shown below.
The values were measured at +25 °C and battery operating conditions.

Table 5: RTC Current Consumption

Mode	Voltage	Current
Intel® Core™ Ultra processor integrated RTC	1.5 V	3 µA

The current consumption of the RTC in the Intel® Core™ Ultra processor Product Family Datasheet is specified with 6 µA in average, but the values measured on several TQMxCU1-HPCM are lower.

3.3 Environmental Conditions

- Operating standard temperature: 0 °C to +60 °C
- Storage temperature: –40 °C to +85 °C
- Relative humidity (operating): 10 % to 90 % (non-condensing)
- Relative humidity (storage): 5 % to 95 % (non-condensing)

Attention: Maximum operating temperature	
	Do not operate the TQMxCU1-HPCM without properly attached heat spreader and heat sink. The heat spreader is not a sufficient heat sink.

3.4 System Components

3.4.1 Processor

The TQMxCU1-HPCM supports the Intel® Core™ Ultra processor series (Meteor Lake).

The following list illustrates some key features of the Intel® Core™ Ultra processor series:

- Intel® hybrid processor design combines Performance-cores with Efficiency–cores, together up to 16 cores
- LPDDR5x speed up to 7467 MT/s
- Intel® 64 Architecture
- Intel® Hyper-Threading Technology (Intel® HT Technology)
- Intel® Advanced Vector Extensions 2 (Intel® AVX2)
- Intel® AVX2 Vector Neural Network Instructions (Intel® AVX2 VNNI)
- Intel® Turbo Boost Max Technology 3.0
- Intel® Configurable Thermal Design Power (Intel® cTDP up and down)
- Intel® Enhanced Intel® SpeedStep® technology
- Intel® Arc Graphics architecture with up to 8Xe / 128 Execution Units (EUs)
- Intel® Neural Processing Unit (NPU) for optimized AI acceleration

Table 6: Intel® Core™ Ultra Processor H-Series 28 W (Intel Spec)

Mode	Intel® Core™ Ultra 7 165H	Intel® Core™ Ultra 7 155H	Intel® Core™ Ultra 5 135H	Intel® Core™ Ultra 5 125H
Processor Cores	6P + 8E + 2LP	6P + 8E + 2LP	4P + 8E + 2LP	4P + 8E + 2LP
No of Threads	22	22	18	18
Cache	24 Mbyte	24 Mbyte	18 Mbyte	18 Mbyte
P-Core Base clock	1.4 GHz	1.4 GHz	1.7 GHz	1.2 GHz
E-Core Base clock	0.9 GHz	0.9 GHz	1.2 GHz	0.7 GHz
LP-Core Base clock	0.7 GHz	0.7 GHz	0.7 GHz	0.7 GHz
P-Core Max. Turbo clock	5.0 GHz	4.8 GHz	4.6 GHz	4.5 GHz
E-Core Max. Turbo clock	3.8 GHz	3.8 GHz	3.6 GHz	3.6 GHz
LP-Core Max. Turbo clock	2.5 GHz	2.5 GHz	2.5 GHz	2.5 GHz
$T_{junction}$	0 °C to +110 °C	0 °C to +110 °C	0 °C to +110 °C	0 °C to +110 °C
Memory speed LPDDR5x	7467 MT/s	7467 MT/s	7467 MT/s	7467 MT/s
Max. memory LPDDR5x	64 Gbyte	64 Gbyte	64 Gbyte	64 Gbyte
Graphics	Intel® Arc® 8Xe	Intel® Arc® 8Xe	Intel® Arc® 7Xe	Intel® Arc® 7Xe
Graphics Execution Units	128	128	112	112
Graphics Turbo clock	2.3 GHz	2.25 GHz	2.2 GHz	2.2 GHz
Configurable Thermal Design Power (cTDP nominal)	28 W	28 W	28 W	28 W
Configurable Thermal Design Power (cTDP down)	20 W	20 W	20 W	20 W
Processor Power Limit 2 (PL2)	64 W	64 W	64 W	64 W
Intel® Hyper-Threading Technology	Yes	Yes	Yes	Yes
vPro	Yes	No	Yes	No
NPU	Yes	Yes	Yes	Yes
Intel® Thunderbolt™ 4	Yes	Yes	Yes	Yes
AI Software Frameworks	OpenVINO™, WindowsML, ONNX RT	OpenVINO™, WindowsML, ONNX RT	OpenVINO™, WindowsML, ONNX RT	OpenVINO™, WindowsML, ONNX RT
CPU Use Condition	Embedded	Embedded	Embedded	Embedded

Note: Intel® Core™ Ultra Processor H-Series cTDP up mode	
	The TQMxCU1-HPCM module does not support the Configurable Thermal Design Power (cTDP) up mode. The maximum module power is limited to 28 W processor power consumption.

Table 7: Intel® Core™ Ultra Processor U-Series 15 W (Intel Spec)

Mode	Intel® Core™ Ultra 7 165U	Intel® Core™ Ultra 7 155U	Intel® Core™ Ultra 5 135U	Intel® Core™ Ultra 5 125U
Processor Cores	2P + 8E + 2LP	2P + 8E + 2LP	2P + 8E + 2LP	2P + 8E + 2LP
No of Threads	14	14	14	14
Cache	12 Mbyte	12 Mbyte	12 Mbyte	12 Mbyte
P-Core Base clock (cTDP nominal)	1.7 GHz	1.7 GHz	1.6 GHz	1.3 GHz
P-Core Base clock (cTDP up)	2.7 GHz	2.7 GHz	2.7 GHz	2.7 GHz
E-Core Base clock	1.2 GHz	1.2 GHz	1.1 GHz	0.8 GHz
LP-Core Base clock	0.7 GHz	0.7 GHz	0.7 GHz	0.7 GHz
P-Core Max. Turbo clock	4.9 GHz	4.8 GHz	4.4 GHz	4.3 GHz
E-Core Max. Turbo clock	3.8 GHz	3.8 GHz	3.6 GHz	3.6 GHz
LP-Core Max. Turbo clock	2.1 GHz	2.1 GHz	2.1 GHz	2.1 GHz
$T_{junction}$	0 °C to +110 °C	0 °C to +110 °C	0 °C to +110 °C	0 °C to +110 °C
Memory speed LPDDR5x	7467 MT/s	7467 MT/s	7467 MT/s	7467 MT/s
Max. memory LPDDR5x	64 Gbyte	64 Gbyte	64 Gbyte	64 Gbyte
Graphics	Intel® Arc® 4Xe	Intel® Arc® 4Xe	Intel® Arc® 4Xe	Intel® Arc® 4Xe
Graphics Execution Units	64	64	64	64
Graphics Turbo clock	2.0 GHz	1.95 GHz	1.9 GHz	1.85 GHz
Thermal Design Power (cTDP nominal)	15 W	15 W	15 W	15 W
Configurable Thermal Design Power (cTDP down)	12 W	12 W	12 W	12 W
Configurable Thermal Design Power (cTDP up)	28 W	28 W	28 W	28 W
Processor Power Limit 2 (PL2)	57 W	57 W	57 W	57 W
Intel® Hyper-Threading Technology	Yes	Yes	Yes	Yes
vPro	Yes	No	Yes	No
NPU	Yes	Yes	Yes	Yes
Intel® Thunderbolt™ 4	Yes	Yes	Yes	Yes
AI Software Frameworks	OpenVINO™, WindowsML, ONNX RT	OpenVINO™, WindowsML, ONNX RT	OpenVINO™, WindowsML, ONNX RT	OpenVINO™, WindowsML, ONNX RT
CPU Use Condition	Embedded	Embedded	Embedded	Embedded

3.4.1.1 Intel® Turbo Boost Technology

Intel® Turbo Boost Technology accelerates processor and graphics performance for peak loads, automatically allowing processor cores to run faster than the rated operating frequency if they are operating within power, current, and temperature specification limits. It depends on the workload and operating environment and the period of time the processor spends in that state whether the processor enters Intel® Turbo Boost.

To maximize performance, the Intel® Turbo Boost Technology allows the processor to operate for short durations at a power level that is higher than its Thermal Design Power (TDP) configuration.

The Intel® Turbo Boost Technology can be configured in the UEFI BIOS; default is “enabled”.

3.4.1.2 Intel® Configurable Thermal Design Power

With the Intel® Configurable Thermal Design Power (cTDP) feature, the processor’s power consumption can be customized.

The cTDP consists of three modes:

1. The cTDP nominal mode specifies the processor rated clock and maximum power consumption.
2. The cTDP down mode specifies a lower maximum processor power consumption and lower guaranteed clock versus the nominal mode. This mode is intended for ultra low-power applications, e.g. systems with limited cooling solutions.
3. The cTDP up mode specifies a higher maximum processor power consumption and a higher guaranteed clock versus the nominal mode. This mode is intended for high performance applications with optimized cooling solutions.

3.4.2 Graphics

The Intel® Core™ Ultra processor features an integrated Intel® HD graphics accelerator.

It provides excellent 2D / 3D graphics performance with support of up to three simultaneous displays.

The following list illustrates some key features of the Intel® Core™ Ultra processor:

- Intel® ARC® 8Xe Graphics with up to 128 Execution Units
- Hardware accelerated video decoding/encoding for H.264 (AV), H.265 (HVEC), AV-1, MPEG, VP9
- DirectX 12.2
- OpenGL 4.6
- OpenCL 3.0
- Single 8K60Hz panel support

The TQMxCU1-HPCM supports three external Digital Display Interfaces (DDI0, DDI1) with DP++ configuration and one internal eDP display interface at the COM-HPC® Mini connector.

The Intel® Core™ Ultra processor supports up to four display streams simultaneously.

3.4.3 Memory

3.4.3.1 LPDDR5x SDRAM

The TQMxCU1-HPCM supports a dual-channel LPDDR5x memory that operates at up to 7460 MT/s.

System memory sizes of 16, 32 or 64 Gbyte are supported.

The Intel® Core™ Ultra processor supports IBECC (In-Band ECC).

3.4.3.2 SPI Boot Flash Interface

The TQMxCU1-HPCM provides a 256 Mbit SPI boot flash. It includes the Intel® Management Engine (Intel® ME) and the UEFI BIOS.

An external SPI boot flash on the carrier can be used instead of the on-board SPI boot flash.

The UEFI BIOS supports the following 1.8 V SPI flash devices on the carrier board:

- Macronix MX25U25643G

3.4.3.3 UEFI BIOS Flash Boot Select Signals

The COM-HPC® Base Specification describes various SPI boot source options.
With BSEL[2:0], the SPI UEFI BIOS boot source can be selected.

Table 8: BIOS Flash Boot Select Signals

BSEL2	BSEL1	BSEL0	Boot
1	1	1	Boot from module SPI UEFI BIOS flash (default)
1	1	0	Boot from carrier SPI UEFI BIOS flash

3.4.3.4 SPI General-purpose Interface

The TQMxCU1-HPCM supports a general-purpose SPI interface. The SPI Master is on the module. The interface may be used with general-purpose SPI devices such as DACs, A/D converters or CAN controller on the carrier.

Please contact TQ-Support for further information about software and device support.

3.4.3.5 EEPROM

The TQMxCU1-HPCM supports a COM-HPC® Mini module EEPROM. The 2 Kbit EEPROM AT24AA32 is connected to the general-purpose I2C0 interface (COM-HPC® Mini pin names: I2C0_DAT and I2C0_CLK).

3.4.4 Real Time Clock

The TQMxCU1-HPCM features a standard RTC integrated in the Intel® Core™ Ultra processor.

3.4.5 Trusted Platform Module

The TQMxCU1-HPCM supports the Trusted Platform Module (TPM) 2.0 with the Infineon SLB9672 controller.
The Intel® Core™ Ultra processor also support a Firmware Trusted Platform Module (fTPM), which is a Trusted Platform Module 2.0 implementation in firmware. This feature can be configured in the BIOS.

3.4.6 Temperature Monitor and Fan Control

The TQMxCU1-HPCM features an integrated Hardware Monitor to monitor the processor die temperature and manage the fan control of the COM-HPC® Mini interface.

3.4.7 TQ Flexible I/O Configuration (TQ-flexiCFG)

The TQ-Systems COM-HPC® Mini module TQMxCU1-HPCM features a flexible I/O configuration feature, TQ-flexiCFG.
Using the TQ-flexiCFG feature, several COM-HPC® Mini I/O interfaces and functions can be configured via a programmable FPGA.
This option allows TQ-Systems to integrate special embedded features and configuration options in the TQMxCU1-HPCM to reduce the carrier board design effort. Some examples of flexible I/O configuration are:

- GPIO interrupt configuration
- Interrupt configuration
- Integration of additional I/O functions,
  (e.g. additional Serial, CAN, I^2C, PWM controller or special power management configurations)

Note: The configuration/adaption of the FPGA cannot be done by the user. All changes have to be implemented by TQ.

Please contact TQ-Support for further information about the TQ-flexiCFG.

3.5 Interfaces

3.5.1 PCI Express Interface

On the COM-HPC® Mini connector, the TQMxCU1-HPCM supports up to 16 × PCI Express Gen4 lanes with 16 Gb/s speed. The PCI Express lane configuration can be defined with a customized BIOS.

Table 9: COM-HPC® Mini PCI Express Group 0 low port 07 – 00 Configuration

Lane	Link			CPU	TX Coupling Cap location	RX Coupling Cap location
07	×1	×2	**×4 (default)**	HSIO 1	On carrier	On carrier
06	×1			HSIO 2	On carrier	On carrier
05	×1	×2		HSIO 3	On carrier	On carrier
04	×1			HSIO 4	On carrier	On carrier
03	**×1 (default)**	×2	×4	HSIO 8 (H-series only) *1)	On carrier	On carrier
02	**×1 (default)**			HSIO 7	On carrier	On carrier
01	**×1 (default)**	×2		HSIO 6	On carrier	On carrier
00	**×1 (default)**			HSIO 5	On carrier	On carrier

*1) The Intel® Core™ Ultra processor U-series supports only 15 PCI Express lanes. Lane 03 is not supported.

PCI Express Lane 07 and 06 can alternatively be used for SATA 0/1. Please contact TQ-Support if you want to use SATA ports.

Table 10: COM-HPC® Mini PCI Express Group 0 high port 15 – 08 Configuration

Lane	Link			CPU	TX Coupling Cap location	RX Coupling Cap location
15			**×4 (default)**	HSIO 20	On module	On carrier
14				HSIO 19	On module	On carrier
13		×2		HSIO 18	On module	On carrier
12	×1			HSIO 17	On module	On carrier
11			**×4 (default)**	HSIO 16	On module	On carrier
10				HSIO 15	On module	On carrier
09		×2		HSIO 14	On module	On carrier
08	×1			HSIO 13	On module	On carrier

3.5.2 DDI / USB4 / USB 3.2 / USB 2.0 Interface

The TQMxCU1-HPCM supports a very flexible configuration of 8 × Super Speed lanes that may be used for DDI, USB4, or USB 3.2 interfaces.

The Super Speed lane 4-7 are configured to four USB 3.2 2x1 ports.

The Super Speed lane 0-1 and 2-3 can be configured to DDI or to a USB Type-C sub-system. The port configuration can be changed with dedicated BIOS versions.

The USB Type-C sub-system supports USB4, DPoC (DisplayPort over Type-C), USB 3.2 2x1 and USB 3.2 2x2 protocols.
The Thunderbolt™ protocol is not supported the official Thunderbolt™ branding requires a certification.

Table 11: COM-HPC® Mini Super Speed Lane 7 – 0 Configuration

Lane	Config 1	Config 2	USB 2.0 support
0	DDI #0	DDI #0	–
1			
2	DDI #1	USB4 #0	USB 2.0 #0
3			
4	USB 3 #3	USB 3 #3	USB 2.0 #1
5	USB 3 #2	USB 3 #2	USB 2.0 #4
6	USB 3 #1	USB 3 #1	USB 2.0 #3
7	USB 3 #0	USB 3 #0	USB 2.0 #5

USB 2.0 lanes 2, 6, and 7 can be used as general-purpose ports; they are not required for USB4 or USB 3.2 support.

The TQMxCU1-HPCM supports eight USB 2.0 and four USB 3.2 Gen 2 ports with data rates of up to 10 Gb/s at the COM-HPC® Mini connector. All USB 3.2 Gen 2 ports are configurable to USB 3.2 Gen 1 (5 Gb/s).
Care must be taken in the COM-HPC® Mini carrier design. The carrier must support the USB 3.2 Gen 2 (10 Gb/s) high-speed standard if you want to use full bandwidth.

Note: USB 3.1 Gen 2 (10 Gb/s) carrier design	
	If the COM-HPC® Mini carrier is not designed for USB 3.2 Gen 2 (10 Gb/s) operation, the USB 3.2 ports should be configured to operate in Gen 1 mode.

3.5.2.1 USB Type-C configuration

The USB Type-C sub-system supports USB4, DPoC (DisplayPort over Type-C), USB 3.2 2x1 and USB 3.2 2x2 protocols.
The Thunderbolt™ protocol is not supported because the official Thunderbolt™ branding requires a certification.
The USB4 port supports the Microsoft 11 USB4 interdomain connections, the Windows 11 USB4 connection manager supports the Ethernet over USB4 interdomain protocol, also known as USB4NET. This enables two USB4 PCs to establish a network connection with a bandwidth of 20 Gbps between each other when connected using a USB4 cable.

The USB Type-C sub-system was tested on the MB-COMHPCM-1 carrier with the following USB Type-C devices:

- USB4 to PCIe M.2 SSD (with ASM2464PD chip)
- USB 3.2 2x2 to PCIe M.2 SSD (with ASM236x chip)
- USB 3.2 1x1 USBStick
- USB Type-C to Display Port Adapter (DP x4)
- USB Type-C docking station with USB 3.2 and DP ALT Mode (DP x2)
- USB4NET 20 Gbps connection to Laptop (on both platforms Windows 11 was installed)

The Super Speed lane 2-3 supports the USB Type-C operation, with the following retimer and USB Power Delivery controller:

- USB Type-C retimer Intel® JHL9040R (Hayden Bridge)
- USB Power Delivery (PD) controller TI TPS65994BH

Table 12: USB Type-C carrier I2C address port mapping

I2C port	address	description
USB_PD_I2C	0x74	I2C clock line between module Embedded Controller master and carrier based USB Power Delivery controller slave
SML0	0x56	SML0 is used to support carrier USB Type-C retimers
SML1	0x21 / 0x25	SML1 is used to support carrier USB Power Delivery (PD) Controller USB Type-C Port 0 / 1

Note: USB Type-C sub-system carrier design	
	To support the USB Type-C sub-system, the carrier must be designed according to the USB Type-C specification with USB Retimer and USB Power Delivery Controller. Please contact TQ-Support to get more information to the Carrier USB Type-C implementation. For further information about implementing DDI, USB4, or USB 3.2 interfaces, refer to the COM-HPC® Mini carrier Design Guide.

3.5.3 Digital Display Interface

The TQMxCU1-HPCM supports up to three Digital Display Interfaces (DDI0, DDI1, and eDP) at the COM-HPC® Mini connector.
The external Digital Display Interface supports Display Port (DP), High Definition Multimedia Interface (HDMI), and Digital Visual Interface (DVI). Any display combination is possible.

Table 13: Maximum Resolution Display Configuration

Display	Maximum Display Resolution
eDP 1.4b	3840 × 2400 @ 120 Hz
DP 1.4a	7680 × 4320 @ 60 Hz
HDMI 2.1	4096 × 2304 @ 60 Hz (HDMI 2.1 TMDS) 7680 × 4320 @ 60 Hz (HDMI2.1 FRL)

For Super Speed configuration, either USB4 #0 or DDI #1 is possible, depending on the BIOS version.

3.5.4 NBASE-T Ethernet

The TQMxCU1-HPCM features two Intel® i226 Ethernet controller with 10/100/1000/2500 Mbps speed.
The Intel® i226 Ethernet controller provides the following features:

- Automatic speed configuration 10 BASE-T / 100 BASE-TX / 1000 BASE-T / 2500 BASE-T
- Automatic MDI/MDIX crossover at all speeds
- Jumbo frames (up to 9 kB)
- 802.1as/1588 conformance
- Reduced power consumption during normal operation
- Energy Efficient Ethernet (EEE)
- Ethernet TSN support

3.5.5 General-Purpose Input/Output

The TQMxCU1-HPCM provides 12 GPIO signals at the COM-HPC® Mini connector.

3.5.6 High Definition Audio Interface

The TQMxCU1-HPCM provides a High Definition Audio (HDA) interface, which supports an audio codec at the COM-HPC® Mini connector. The Audio Codec hat to be placed on the carrier board.
Please contact TQ-Support to check if your codec is supported by default (BIOS verb table…).

3.5.7 eSPI Bus

The TQMxCU1-HPCM supports the Enhanced Serial Peripheral (eSPI) interface on the COM-HPC® Mini connector pins for general-purpose carrier board devices such as Super I/O and FPGAs.
Please contact TQ-Support for further information about the Serial Peripheral eSPI BIOS and carrier integration.

3.5.8 I²C Bus

The TQMxCU1-HPCM supports three general-purpose I²C port controller integrated in the TQ-flexiCFG block and via the Intel® Core™ Ultra processor. The I²C host controller supports up to 400 kHz and can be configured independently.

- I2C0: integrated in the TQ-flexiCFG block
- I2C1: via the Intel® Core™ Ultra processor I2C1
- I2C2: via the Intel® Core™ Ultra processor I2C2

On the carrier, the I2C should be used for connection I2C devices, the TQ-Systems EAPI supports only the I2C0 port.
The I2C1 and I2C2 port are only supported with the Intel driver package.

3.5.9 SMBus

The TQMxCU1-HPCM provides a System Management Bus (SMBus) via the Intel® Core™ Ultra processor.

3.5.10 Serial Ports

The TQMxCU1-HPCM offers a dual Universal Asynchronous Receiver and Transmitter (UART) controller. The register set is based on the industry standard 16550 UART. The UART operates with standard serial port drivers without requiring a custom driver to be installed. The 16 byte transmit and receive FIFOs reduce CPU overhead and minimize the risk of buffer overflow and data loss.

3.5.11 Watchdog Timer

The TQMxCU1-HPCM supports an independently programmable two-stage Watchdog timer integrated in the TQ-flexiCFG block.
There are four operation modes available for the Watchdog timer:

- Dual-stage mode
- Interrupt mode
- Reset mode
- Timer mode

The Watchdog timer timeout ranges from 125 msec to 1 hour.

Note: Once the watchdog is enabled, the application cannot disable it. Only a system reset can disable the watchdog.
The COM-HPC® Mini Specification provides a hardware strobe option (WD_STROBE# signal) and a Watchdog output indication that a watchdog time-out event has occurred (WD_OUT signal).

3.6 Connectors

3.6.1 COM-HPC® Mini Connector

COM-HPC® Mini modules use one high performance 400-pin connector, introduced by Samtec but is now available from several vendors. This connector (J1) is broken down into four rows: A, B, C, and D.
Two connector versions with 5 mm and 10 mm stack height are available. The connector on the carrier board determines the stack height.

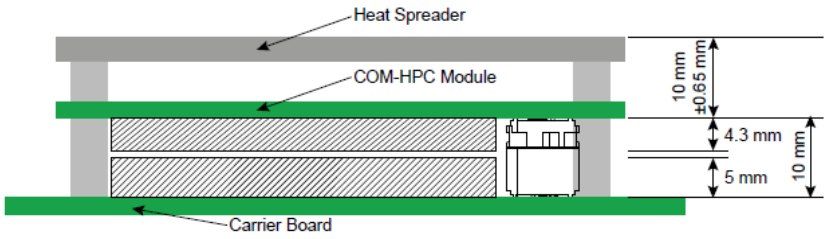

Figure 2: COM-HPC® Mini Vertical Cross Sections – Carrier PCB Top to HSP Top

3.6.2 Debug Header

The TQMxCU1-HPCM features a 14-pin flat cable connector to connect an external debug module (TQ specific) providing UEFI BIOS POST code information, debug LEDs and a JTAG interface for on-board FPGA.
The TQM debug card can be connected at this header.

3.6.3 TQM Debug Card

The TQM debug card is available only upon special request (not a standard accessory). It visualizes several processor and chipset control signals. When the TQMxCU1-HPCM is powered up, the UEFI BIOS POST codes are shown.
If the TQMxCU1-HPCM does not boot, the UEFI BIOS POST has detected a fatal error and stopped.
The number displayed on the TQM debug card is the number of the test step, where the UEFI BIOS boot failed.

Figure 3: TQM Debug Card

Please contact TQ-Support for more details and ordering information about the TQM debug card.

3.6.4 Debug Module LED

The TQMxCU1-HPCM features a dual colour LED, providing boot and BIOS information.
The following table illustrates some LED boot messages:

Table 14: LED Boot Messages

Red LED	Green LED	Remark
ON	OFF	Power supply error
ON	ON	S4/S5 state
Blinking	Blinking	S3 state
OFF	Blinking	UEFI BIOS is booting
OFF	ON	UEFI BIOS boot is completed

Figure 4: Debug Module LED

3.7 COM-HPC® Mini Connector Pinout

This section describes the TQMxCU1-HPCM COM-HPC® Mini connector pin-assignment, which is compliant with COM-HPC® Mini (COM-HPC® Module Base Specification Rev. 1.2).

The COM-HPC® Mini pinout is different and incompatible to the COM-HPC® Client and COM-HPC® Server pinouts.

COM-HPC® Mini I/O voltages:
The COM-HPC® Mini redefines a number of I/O voltage rails from 3.3 V to 1.8 V, reflecting current chipset and SOC trends. Low-speed, single-ended signals, that are directly attached to the chipset and SOC are redefined on the COM-HPC® Mini to operate at 1.8 V.

3.7.1 Signal Assignment Abbreviations

The following table lists the abbreviations used within this chapter:

Table 15: Signal Assignment Abbreviations

Abbreviation	Description
GND	Ground
Power	Power
I	Input
I PU	Input with pull-up resistor
I PD	Input with pull-down resistor
O	Output
O PU	Output with pull-up resistor
O PD	Output with pull-down resistor
OD	Output Open drain
OD PU	Output Open drain with pull-up resistor
I/O	Bi-directional

Note: Unused signals on the carrier board	
	Unused inputs at the COM-HPC® Mini connector can be left open on the carrier board, as these signals are terminated on the TQMxCU1-HPCM.

3.7.2 COM-HPC® Mini Connector Pin Assignment

Table 16: COM-HPC® Mini Connector Pin Assignment

Pin	Pin-Signal	Description	Type	Remark
A1	VCC_1	VCC Primary power input	Power	
A2	VCC_2	VCC Primary power input	Power	
A3	VCC_3	VCC Primary power input	Power	
A4	VCC_4	VCC Primary power input	Power	
A5	RAPID_SHUTDOWN	Rapid shutdown signal to module	I	NC 5.0 V
A6	FUSA_SPI_ALERT	Active high alert output from the COM-HPC Module	O PU	NC
A7	FUSA_STATUS0	Two bit FuSa status / error indication outputs	O PU	NC
A8	FUSA_STATUS1	Two bit FuSa status / error indication outputs	O PD	NC
A9	PCIe_PERST_IN0#	Reset signals into Module to reset Module PCIe Targets	I	NC
A10	GND_1	Ground	GND	
A11	PCIe_REFCLKIN0–	Reference clock input	I	NC
A12	PCIe_REFCLKIN0+	Reference clock input	I	NC
A13	GND_2	Ground	GND	
A14	USB7–	USB differential pair	IO	
A15	USB7+	USB differential pair	IO	
A16	GND_3	Ground	GND	
A17	USB6–	USB differential pair	IO	
A18	USB6+	USB differential pair	IO	
A19	GND_4	Ground	GND	
A20	SS23_SDA_AUX–	HDMI I2C / DisplayPort Aux	IO	
A21	SS23_SCL_AUX+	HDMI I2C / DisplayPort Aux	IO	
A22	GND_5	Ground	GND	
A23	SS2_TX–	Super Speed differential pair	O	
A24	SS2_TX+	Super Speed differential pair	O	
A25	GND_6	Ground	GND	
A26	SS2_RX–	Super Speed differential pair	I	
A27	SS2_RX+	Super Speed differential pair	I	
A28	GND_7	Ground	GND	
A29	SS3_TX–	Super Speed differential pair	O	
A30	SS3_TX+	Super Speed differential pair	O	
A31	GND_8	Ground	GND	
A32	SS3_RX–	Super Speed differential pair	I	
A33	SS3_RX+	Super Speed differential pair	I	
A34	GND_9	Ground	GND	
A35	eDP_AUX–	eDisplayPort Aux	IO	
A36	eDP_AUX+	eDisplayPort Aux	IO	
A37	GND_10	Ground	GND	
A38	eDP_TX0–	eDisplayPort differential pair	O	
A39	eDP_TX0+	eDisplayPort differential pair	O	
A40	GND_11	Ground	GND	
A41	eDP_TX1–	eDisplayPort differential pair	O	
A42	eDP_TX1+	eDisplayPort differential pair	O	
A43	GND_12	Ground	GND	
A44	eDP_TX2–	eDisplayPort differential pair	O	
A45	eDP_TX2+	eDisplayPort differential pair	O	
A46	GND_13	Ground	GND	
A47	eDP_TX3–	eDisplayPort differential pair	O	
A48	eDP_TX3+	eDisplayPort differential pair	O	
A49	GND_14	Ground	GND	

COM-HPC® Mini Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
A50	eSPI_IO0	eSPIO I/O signal	IO	
A51	eSPI_IO1	eSPIO I/O signal	IO	
A52	eSPI_IO2	eSPIO I/O signal	IO	
A53	eSPI_IO3	eSPIO I/O signal	IO	
A54	eSPI_CLK	eSPIO clock signal	O	
A55	GND_15	Ground	GND	
A56	PCIe_CLKREQ0_LO#	PCIe reference clock low request signal from Carrier	IO PU	
A57	PCIe_CLKREQ0_HI#	PCIe reference clock high request signal from Carrier	IO PU	
A58	PCIe_CLKREQ_OUT0#	PCIe reference clock request from Module target PCIe device	IO PU	NC
A59	NBASET1_LINK_MAX#	NBASE-T Ethernet Controller 1 MAX Speed Link indicator, active low	O	3.3 V
A60	NBASET1_CTREF	Reference voltage for Carrier Board NBASET Ethernet 1	O	
A61	GND_16	Ground	GND	
A62	PCIe08_TX–	PCI Express high differential pair	O	
A63	PCIe08_TX+	PCI Express high differential pair	O	
A64	GND_17	Ground	GND	
A65	PCIe09_TX–	PCI Express high differential pair	O	
A66	PCIe09_TX+	PCI Express high differential pair	O	
A67	GND_18	Ground	GND	
A68	PCIe10_TX–	PCI Express high differential pair	O	
A69	PCIe10_TX+	PCI Express high differential pair	O	
A70	GND_19	Ground	GND	
A71	PCIe11_TX–	PCI Express high differential pair	O	
A72	PCIe11_TX+	PCI Express high differential pair	O	
A73	GND_20	Ground	GND	
A74	PCIe12_TX–	PCI Express high differential pair	O	
A75	PCIe12_TX+	PCI Express high differential pair	O	
A76	GND_21	Ground	GND	
A77	PCIe13_TX–	PCI Express high differential pair	O	
A78	PCIe13_TX+	PCI Express high differential pair	O	
A79	GND_22	Ground	GND	
A80	PCIe14_TX–	PCI Express high differential pair	O	
A81	PCIe14_TX+	PCI Express high differential pair	O	
A82	GND_23	Ground	GND	
A83	PCIe15_TX–	PCI Express high differential pair	O	
A84	PCIe15_TX+	PCI Express high differential pair	O	
A85	GND_24	Ground	GND	
A86	VCC_RTC	RTC power input	Power	
A87	SUS_CLK	32.768 kHz clock used by Carrier peripherals	O PD	
A88	GPIO_00	General purpose input / output pin default input	IO PU	
A89	GPIO_01	General purpose input / output pin default input	IO PU	
A90	GPIO_02	General purpose input / output pin default input	IO PU	
A91	GPIO_03	General purpose input / output pin default input	IO PU	
A92	GPIO_04	General purpose input / output pin default input	IO PU	
A93	GPIO_05	General purpose input / output pin default input	IO PU	
A94	GPIO_06	General purpose input / output pin default input	IO PU	
A95	GPIO_07	General purpose input / output pin default input	IO PU	
A96	GPIO_08	General purpose input / output pin default input	IO PU	
A97	GPIO_09	General purpose input / output pin default input	IO PU	
A98	GPIO_10	General purpose input / output pin default input	IO PU	
A99	GPIO_11	General purpose input / output pin default input	IO PU	
A100	PINOUT_TYPE0	NC Mini Module – Wide Range 8V to 20V input	O	NC

COM-HPC® Mini Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
B1	VCC_5	VCC Primary power input	Power	
B2	PWRBTN#	power button input	I PU	
B3	VCC_6	VCC Primary power input	Power	
B4	THERMTRIP#	Active low out indicating that the CPU has entered thermal shutdown	O	
B5	CAN_TX	CAN bus 1.8V logic level transmit signal	O	NC
B6	TAMPER#	Tamper or Intrusion detection line on VCC_RTC power well	I PU	
B7	PROCHOT#	Active low output indicating a temperature hot event on module	O	
B8	SUS_S3#	Indicates system is in Suspend to RAM (S3)	O PD	
B9	FUSA_VOLTAGE_ERR#	Active low output indicating an over- or under voltage error	O PU	NC
B10	WD_STROBE#	Strobe input to watchdog timer. Periodic strobing prevents the watchdog	I PU	
B11	WD_OUT	Output indicating that a watchdog time-out event has occurred	O	
B12	GND_25	Ground	GND	
B13	USB5–	USB differential pair	IO	
B14	USB5+	USB differential pair	IO	
B15	GND_26	Ground	GND	
B16	USB4–	USB differential pair	IO	
B17	USB4+	USB differential pair	IO	
B18	GND_27	Ground	GND	
B19	I2S_LRCLK/SNDW_CLK3/HDA_SYNC	HDA sample synchronization signal	O	optional I2S
B20	I2S_DOUT/SNDW_DAT3/HDA_SDO	HDA serial TDM data output	O	optional I2S
B21	I2S_MCLK/HDA_RST#	HDA reset output	O	optional I2S
B22	I2S_DIN/SNDW_DAT2/HDA_SDI	HDA serial TDM data input	I	optional I2S
B23	I2S_CLK/SNDW_CLK2/HDA_BCLK	HDA serial data clock	O	optional I2S
B24	RSVD	Reserved	–	NC
B25	USB67_OC#	USB overcurrent status	I PU	
B26	USB45_OC#	USB overcurrent status	I PU	
B27	USB23_OC#	USB overcurrent status	I PU	
B28	USB01_OC#	USB overcurrent status	I PU	
B29	SML1_CLK	I2C data based System Management Link	O PU	
B30	SML1_DAT	I2C data based System Management Link	IO PU	
B31	PMCALERT#	Active low Alert signal associated with the SML1 System Management link	I PU	
B32	SML0_CLK	I2C data based System Management Link	O PU	
B33	SML0_DAT	I2C data based System Management Link	IO PU	
B34	USB_PD_ALERT#	Active low Alert signal from USB Power Delivery Controller to the Module	I PU	
B35	USB_PD_I2C_CLK	I2C data line between Module based Embedded Controller	O PU	
B36	USB_PD_I2C_DAT	I2C data line between Module based Embedded Controller	IO PU	
B37	USB_RT_ENA	Power Enable for Carrier based USB Retimers	O	
B38	USB3_LSRX	Sideband RX interface for USB4 Alternate modes	I PD	NC
B39	USB3_LSTX	Sideband TX interface for USB4 Alternate modes	O	NC
B40	USB2_LSRX/DDI0_DDC_AUX_SEL	Sideband RX interface for USB4 Alternate modes / DP AUX select input	I PD	
B41	USB2_LSTX/DDI0_HPD	Sideband TX interface for USB4 Alternate modes / DP Hot Plug detect	IO PD	
B42	GND_28	Ground	GND	
B43	USB1_AUX–	DisplayPort Aux channel for USB4 DP modes	I/O	NC
B44	USB1_AUX+	DisplayPort Aux channel for USB4 DP modes	I/O	NC
B45	LID#	Low active signal for a LID switch	I PU	
B46	SLEEP#	Low active signal for a SLEEP signal	I PU	
B47	VCC_BOOT_SPI	Power supply for Carrier Board SPI – sourced from Module	Power	1.8 V
B48	BOOT_SPI_CS#	Boot SPI chip select for Carrier board SPI flash chip	O	
B49	BSEL0	BIOS Boot select signals	I PU	

COM-HPC® Mini Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
B50	BSEL1	BIOS Boot select signals	I PU	
B51	BSEL2	BIOS Boot select signals	I PU	
B52	eSPI_ALERT0#	eSPI Alert signal	I PU	
B53	eSPI_ALERT1#	eSPI Alert signal	I PU	NC
B54	eSPI_CS0#	eSPI chip select signal	O	
B55	eSPI_CS1#	eSPI chip select signal	O	NC
B56	eSPI_RST#	eSPI reset signal	O	
B57	PCIe_WAKE_OUT0#	Wake request signal from Module based PCIe Target to an	OD PU	NC
B58	NBASET1_LINK_MID#	NBASE-T Ethernet Controller 1 MID Speed Link indicator, active low	O	3.3 V
B59	NBASET1_LINK_ACT#	NBASE-T Ethernet Controller 1 activity indicator, active low	O	3.3 V
B60	GND_29	Ground	GND	
B61	PCIe08_RX–	PCI Express high differential pair	I	
B62	PCIe08_RX+	PCI Express high differential pair	I	
B63	GND_30	Ground	GND	
B64	PCIe09_RX–	PCI Express high differential pair	I	
B65	PCIe09_RX+	PCI Express high differential pair	I	
B66	GND_31	Ground	GND	
B67	PCIe10_RX–	PCI Express high differential pair	I	
B68	PCIe10_RX+	PCI Express high differential pair	I	
B69	GND_32	Ground	GND	
B70	PCIe11_RX–	PCI Express high differential pair	I	
B71	PCIe11_RX+	PCI Express high differential pair	I	
B72	GND_33	Ground	GND	
B73	PCIe12_RX–	PCI Express high differential pair	I	
B74	PCIe12_RX+	PCI Express high differential pair	I	
B75	GND_34	Ground	GND	
B76	PCIe13_RX–	PCI Express high differential pair	I	
B77	PCIe13_RX+	PCI Express high differential pair	I	
B78	GND_35	Ground	GND	
B79	PCIe14_RX–	PCI Express high differential pair	I	
B80	PCIe14_RX+	PCI Express high differential pair	I	
B81	GND_36	Ground	GND	
B82	PCIe15_RX–	PCI Express high differential pair	I	
B83	PCIe15_RX+	PCI Express high differential pair	I	
B84	GND_37	Ground	GND	
B85	TEST#	Module input to allow vendor specific Module test mode	I PU	
B86	RSMRST_OUT#	This is a buffered copy of the internal Module RSMRST	O PD	
B87	UART1_TX	Logic level asynchronous serial port transmit signal	O	
B88	UART1_RX	Logic level asynchronous serial port receive signal	I	
B89	UART1_RTS#	Logic level asynchronous serial port Request to Send signal	O	
B90	UART1_CTS#	Logic level asynchronous serial port Clear to Send signal	I	
B91	I2C2_CLK/ETH_MDIO_CLK	general purpose I2C2 port	O PU	
B92	I2C2_DAT/ETH_MDIO_DAT	general purpose I2C2 port	IO PU	
B93	GP_SPI_MOSI	General Purpose SPI Port Serial data from the Module to the Carrier	O	
B94	GP_SPI_MISO	General Purpose SPI Port Serial data into the Module from the Carrier	I	
B95	GP_SPI_CS0#	General Purpose SPI Port chip select signal	O	
B96	GP_SPI_CS1#	General Purpose SPI Port chip select signal	O	NC
B97	GP_SPI_CS2#	General Purpose SPI Port chip select signal	O	NC
B98	GP_SPI_CS3#	General Purpose SPI Port chip select signal	O	NC
B99	GP_SPI_CLK	General Purpose SPI Port clock signal	O	
B100	GP_SPI_ALERT#	General Purpose SPI Port Alert signal	I PU	

COM-HPC® Mini Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
C1	VCC_7	VCC Primary power input	Power	
C2	RSTBTN#	Reset button input	I PU	
C3	VCC_8	VCC Primary power input	Power	
C4	CARRIER_HOT#	Input from Module temp sensor indicating a too high temperature	I PU	
C5	CAN_RX	CAN bus 1.8V logic level receive signal	I	NC
C6	VIN_PWR_OK	Power OK from main power supply. A high value indicates that the power is good.	I PU	1.8 V
C7	CATERR#	–	–	
C8	SUS_S4_S5#	Indicates system is in Suspend to Disk (S4) or Soft Off (S5) state	O PD	
C9	FUSA_ALERT#	Active low Alert output from the COM-HPC Module	O PU	NC
C10	BATLOW#	Indicates that external battery is low	I PU	
C11	FAN_PWMOUT	Fan speed control for system fan	O	
C12	FAN_TACHIN	Fan tachometer input for a fan with a two pulse per revolution output	I PU	
C13	GND_38	Ground	GND	
C14	USB3–	USB differential pair	IO	
C15	USB3+	USB differential pair	IO	
C16	GND_39	Ground	GND	
C17	USB2–	USB differential pair	IO	
C18	USB2+	USB differential pair	IO	
C19	GND_40	Ground	GND	
C20	SNDW_DMIC_CLK1	Clock for Soundwire transactions	IO	
C21	SNDW_DMIC_DAT1	Bidirectional PCM audio data	O	
C22	GND_41	Ground	GND	
C23	SNDW_DMIC_CLK0	Clock for Soundwire transactions	IO	
C24	SNDW_DMIC_DAT0	Bidirectional PCM audio data	O	
C25	GND_42	Ground	GND	
C26	USB0_LSRX/DDI1_DDC_AUX_SEL	Sideband RX interface for USB4 Alternate modes / DP AUX select input	I PD	
C27	USB1_LSRX	Sideband RX interface for USB4 Alternate modes	I PD	NC
C28	USB0_LSTX/DDI1_HPD	Sideband TX interface for USB4 Alternate modes / DP Hot Plug detect	IO PD	
C29	USB1_LSTX	Sideband TX interface for USB4 Alternate modes	O	NC
C30	eDP_HPD	eDP Hot Plug detect	I PD	
C31	eDP_VDD_EN	eDP power enable	O PD	
C32	eDP_BKLT_EN	eDP backlight enable	O PD	
C33	eDP_BKLTCTL	eDP backlight brightness control	O PD	
C34	GND_43	Ground	GND	
C35	USB3_AUX–	DisplayPort Aux channel for USB4 DP modes	IO	NC
C36	USB3_AUX+	DisplayPort Aux channel for USB4 DP modes	IO	NC
C37	GND_44	Ground	GND	
C38	SS6_RX–	Super Speed differential pair	I	
C39	SS6_RX+	Super Speed differential pair	I	
C40	GND_45	Ground	GND	
C41	SS7_RX–	Super Speed differential pair	I	
C42	SS7_RX+	Super Speed differential pair	I	
C43	GND_46	Ground	GND	
C44	SS4_RX–	Super Speed differential pair	I	
C45	SS4_RX+	Super Speed differential pair	I	
C46	GND_47	Ground	GND	
C47	SS5_RX–	Super Speed differential pair	I	
C48	SS5_RX+	Super Speed differential pair	I	
C49	GND_48	Ground	GND	

COM-HPC® Mini Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
C50	BOOT_SPI_IO0	Boot SPI IO0 signal for Carrier board SPI flash chip	IO	
C51	BOOT_SPI_IO1	Boot SPI IO0 signal for Carrier board SPI flash chip	IO	
C52	BOOT_SPI_IO2	Boot SPI IO0 signal for Carrier board SPI flash chip	IO	
C53	BOOT_SPI_IO3	Boot SPI IO0 signal for Carrier board SPI flash chip	IO	
C54	BOOT_SPI_CLK	Boot SPI clock signal for Carrier board SPI flash chip	O	
C55	GND_49	Ground	GND	
C56	PCIe_REFCLK0_HI–	Reference clock pair for PCIe lanes [15:8] high	O	
C57	PCIe_REFCLK0_HI+	Reference clock pair for PCIe lanes [15:8] high	O	
C58	GND_50	Ground	GND	
C59	PCIe_REFCLK0_LO–	Reference clock pair for PCIe lanes [7:0] low	O	
C60	PCIe_REFCLK0_LO+	Reference clock pair for PCIe lanes [7:0] low	O	
C61	GND_51	Ground	GND	
C62	PCIe00_RX–	PCI Express high differential pair	I	
C63	PCIe00_RX+	PCI Express high differential pair	I	
C64	GND_52	Ground	GND	
C65	PCIe01_RX–	PCI Express high differential pair	I	
C66	PCIe01_RX+	PCI Express high differential pair	I	
C67	GND_53	Ground	GND	
C68	PCIe02_RX–/SGMII1_RX–	PCI Express high differential pair	I	
C69	PCIe02_RX+/SGMII1_RX+	PCI Express high differential pair	I	
C70	GND_54	Ground	GND	
C71	PCIe03_RX–/SGMII0_RX–	PCI Express high differential pair	I	
C72	PCIe03_RX+/SGMII0_RX+	PCI Express high differential pair	I	
C73	GND_55	Ground	GND	
C74	PCIe04_RX–	PCI Express high differential pair	I	
C75	PCIe04_RX+	PCI Express high differential pair	I	
C76	GND_56	Ground	GND	
C77	PCIe05_RX–	PCI Express high differential pair	I	
C78	PCIe05_RX+	PCI Express high differential pair	I	
C79	GND_57	Ground	GND	
C80	PCIe06_RX–/SATA1_RX–	PCI Express high differential pair	I	
C81	PCIe06_RX+/SATA1_RX+	PCI Express high differential pair	I	
C82	GND_58	Ground	GND	
C83	PCIe07_RX–/SATA0_RX–	PCI Express high differential pair	I	
C84	PCIe07_RX+/SATA0_RX+	PCI Express high differential pair	I	
C85	GND_59	Ground	GND	
C86	SMB_CLK	System Management Bus bidirectional clock signal	IO PU	
C87	SMB_DAT	System Management Bus bidirectional data signal	IO PU	
C88	SMB_ALERT#	System Management Bus Alert – active low input	I PU	
C89	UART0_TX	Logic level asynchronous serial port transmit signal	O	
C90	UART0_RX	Logic level asynchronous serial port receive signal	I	
C91	UART0_RTS#	Logic level asynchronous serial port Request to Send signal	O	
C92	UART0_CTS#	Logic level asynchronous serial port Clear to Send signal	I	
C93	I2C0_CLK	general purpose I2C0 port	O PU	
C94	I2C0_DAT	general purpose I2C0 port	IO PU	
C95	I2C0_ALERT#	general purpose I2C0 Alert signal	I PU	
C96	I2C1_CLK	general purpose I2C1 port	O PU	
C97	I2C1_DAT	general purpose I2C1 port	IO PU	
C98	NBASET0_SDP	NBASE-T Ethernet Controller 0 Software-Definable Pin	IO	3.3 V
C99	NBASET0_CTREF	Reference voltage for Carrier Board NBASET Ethernet	O	
C100	PINOUT_TYPE1	NC Mini Module – Wide Range 8V to 20V input	O	NC

COM-HPC® Mini Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
D1	VCC_9	VCC Primary power input	Power	
D2	VCC_10	VCC Primary power input	Power	
D3	VCC_11	VCC Primary power input	Power	
D4	VCC_12	VCC Primary power input	Power	
D5	PLTRST#	Platform Reset: output from Module to Carrier Board	O PD	
D6	FUSA_SPI_CS#	Active low chip select into the Module from the Carrier	I	NC
D7	FUSA_SPI_CLK	Clock into the Module from the Carrier	I	NC
D8	FUSA_SPI_MISO	Serial data into the Carrier FuSa SPI Master from the Module	O PU	NC
D9	FUSA_SPI_MOSI	Serial data from the Carrier FuSa SPI Master, into the Module	I	NC
D10	WAKE0#	PCI Express wake up signal	I PU	
D11	WAKE1#	General purpose wake up signal	I PU	
D12	GND_60	Ground	GND	
D13	USB1–	USB differential pair	IO	
D14	USB1+	USB differential pair	IO	
D15	GND_61	Ground	GND	
D16	USB0–	USB differential pair	IO	
D17	USB0+	USB differential pair	IO	
D18	GND_62	Ground	GND	
D19	SS01_SDA_AUX–	HDMI I2C / DisplayPort Aux	IO	
D20	SS01_SCL_AUX+	HDMI I2C / DisplayPort Aux	IO	
D21	GND_63	Ground	GND	
D22	SS0_TX–	Super Speed differential pair	O	
D23	SS0_TX+	Super Speed differential pair	O	
D24	GND_64	Ground	GND	
D25	SS0_RX–	Super Speed differential pair	I	
D26	SS0_RX+	Super Speed differential pair	I	
D27	GND_65	Ground	GND	
D28	SS1_TX–	Super Speed differential pair	O	
D29	SS1_TX+	Super Speed differential pair	O	
D30	GND_66	Ground	GND	
D31	SS1_RX–	Super Speed differential pair	I	
D32	SS1_RX+	Super Speed differential pair	I	
D33	GND_67	Ground	GND	
D34	ACPRESENT	Driven hard low on Carrier if system AC power is not present	I PU	
D35	NBASET1_SDP	NBASE-T Ethernet Controller 1 Software-Definable Pin	IO	3.3 V
D36	GND_68	Ground	GND	
D37	SS6_TX–	Super Speed differential pair	O	
D38	SS6_TX+	Super Speed differential pair	O	
D39	GND_69	Ground	GND	
D40	SS7_TX–	Super Speed differential pair	O	
D41	SS7_TX+	Super Speed differential pair	O	
D42	GND_70	Ground	GND	
D43	SS4_TX–	Super Speed differential pair	O	
D44	SS4_TX+	Super Speed differential pair	O	
D45	GND_71	Ground	GND	
D46	SS5_TX–	Super Speed differential pair	O	
D47	SS5_TX+	Super Speed differential pair	O	
D48	GND_72	Ground	GND	

COM-HPC® Mini Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
D49	NBASET1_MDI0–	Ethernet Controller 1: Media Dependent Interface Differential Pair	IO	
D50	NBASET1_MDI0+	Ethernet Controller 1: Media Dependent Interface Differential Pair	IO	
D51	GND_73	Ground	GND	
D52	NBASET1_MDI1–	Ethernet Controller 1: Media Dependent Interface Differential Pair	IO	
D53	NBASET1_MDI1+	Ethernet Controller 1: Media Dependent Interface Differential Pair	IO	
D54	GND_74	Ground	GND	
D55	NBASET1_MDI2–	Ethernet Controller 1: Media Dependent Interface Differential Pair	IO	
D56	NBASET1_MDI2+	Ethernet Controller 1: Media Dependent Interface Differential Pair	IO	
D57	GND_75	Ground	GND	
D58	NBASET1_MDI3–	Ethernet Controller 1: Media Dependent Interface Differential Pair	IO	
D59	NBASET1_MDI3+	Ethernet Controller 1: Media Dependent Interface Differential Pair	IO	
D60	GND_76	Ground	GND	
D61	PCIe00_TX–	PCI Express high differential pair	O	
D62	PCIe00_TX+	PCI Express high differential pair	O	
D63	GND_77	Ground	GND	
D64	PCIe01_TX–	PCI Express high differential pair	O	
D65	PCIe01_TX+	PCI Express high differential pair	O	
D66	GND_78	Ground	GND	
D67	PCIe02_TX– / SGMII1_TX–	PCI Express high differential pair	O	
D68	PCIe02_TX+ / SGMII1_TX+	PCI Express high differential pair	O	
D69	GND_79	Ground	GND	
D70	PCIe03_TX– / SGMII0_TX–	PCI Express high differential pair	O	
D71	PCIe03_TX+ / SGMII0_TX+	PCI Express high differential pair	O	
D72	GND_80	Ground	GND	
D73	PCIe04_TX–	PCI Express high differential pair	O	
D74	PCIe04_TX+	PCI Express high differential pair	O	
D75	GND_81	Ground	GND	
D76	PCIe05_TX–	PCI Express high differential pair	O	
D77	PCIe05_TX+	PCI Express high differential pair	O	
D78	GND_82	Ground	GND	
D79	PCIe06_TX– / SATA1_TX–	PCI Express high differential pair	O	
D80	PCIe06_TX+ / SATA1_TX+	PCI Express high differential pair	O	
D81	GND_83	Ground	GND	
D82	PCIe07_TX– / SATA0_TX–	PCI Express high differential pair	O	
D83	PCIe07_TX+ / SATA0_TX+	PCI Express high differential pair	O	
D84	GND_84	Ground	GND	
D85	NBASET0_MDI0–	Ethernet Controller 0: Media Dependent Interface Differential Pair	IO	
D86	NBASET0_MDI0+	Ethernet Controller 0: Media Dependent Interface Differential Pair	IO	
D87	GND_85	Ground	GND	
D88	NBASET0_MDI1–	Ethernet Controller 0: Media Dependent Interface Differential Pair	IO	
D89	NBASET0_MDI1+	Ethernet Controller 0: Media Dependent Interface Differential Pair	IO	
D90	GND_86	Ground	GND	
D91	NBASET0_MDI2–	Ethernet Controller 0: Media Dependent Interface Differential Pair	IO	
D92	NBASET0_MDI2+	Ethernet Controller 0: Media Dependent Interface Differential Pair	IO	
D93	GND_87	Ground	GND	
D94	NBASET0_MDI3–	Ethernet Controller 0: Media Dependent Interface Differential Pair	IO	
D95	NBASET0_MDI3+	Ethernet Controller 0: Media Dependent Interface Differential Pair	IO	
D96	GND_88	Ground	GND	
D97	NBASET0_LINK_MAX#	NBASE-T Ethernet Controller 0 MAX Speed Link indicator, active low	O	3.3 V
D98	NBASET0_LINK_MID#	NBASE-T Ethernet Controller 0 MID Speed Link indicator, active low	O	3.3 V
D99	NBASET0_LINK_ACT#	NBASE-T Ethernet Controller 0 activity indicator, active low	O	3.3 V
D100	PINOUT_TYPE2	NC Mini Module – Wide Range 8V to 20V input	O	NC

4. MECHANICS

4.1 Dimensions

The TQMxCU1-HPCM has dimensions of 95 mm × 70 mm (±0.2 mm).
The following figure shows the TQMxCU1-HPCM in a three view.

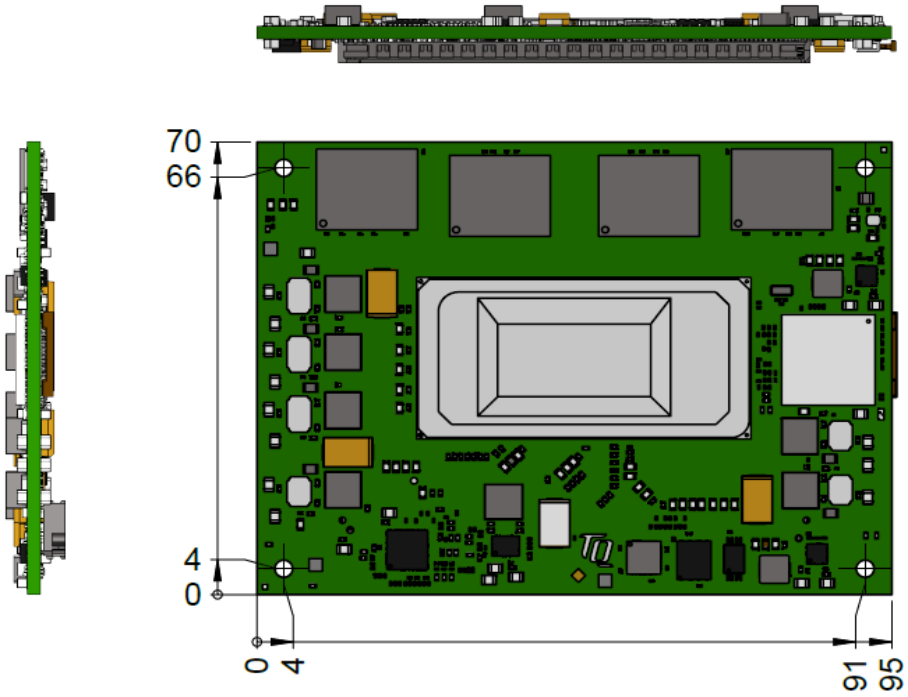

Figure 5: TQMxCU1-HPCM Three View

The following illustration shows the TQMxCU1-HPCM bottom view.

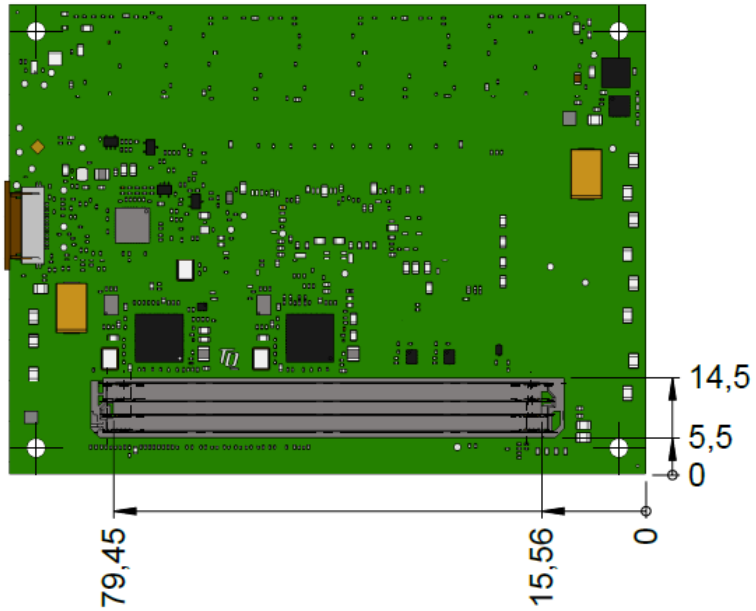

Figure 6: TQMxCU1-HPCM Bottom View

4.2 Component Placement and Labels

The following illustration shows the TQMxCU1-HPCM component placement.

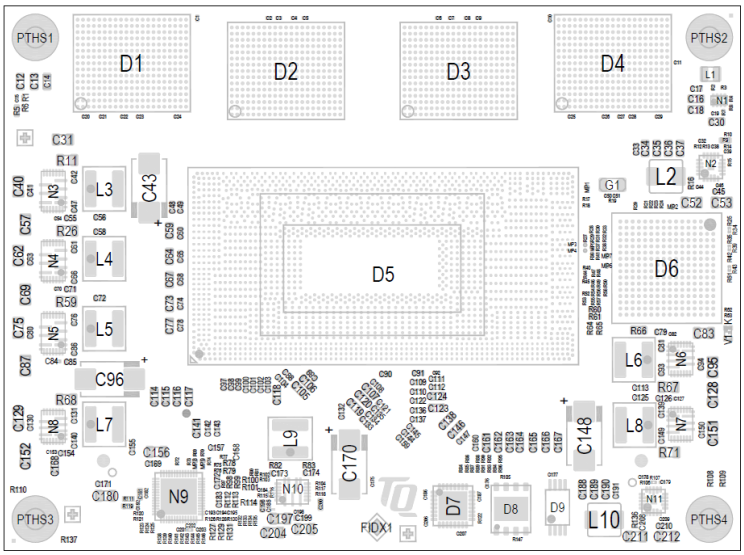

Figure 7: TQMxCU1-HPCM Component Placement Top

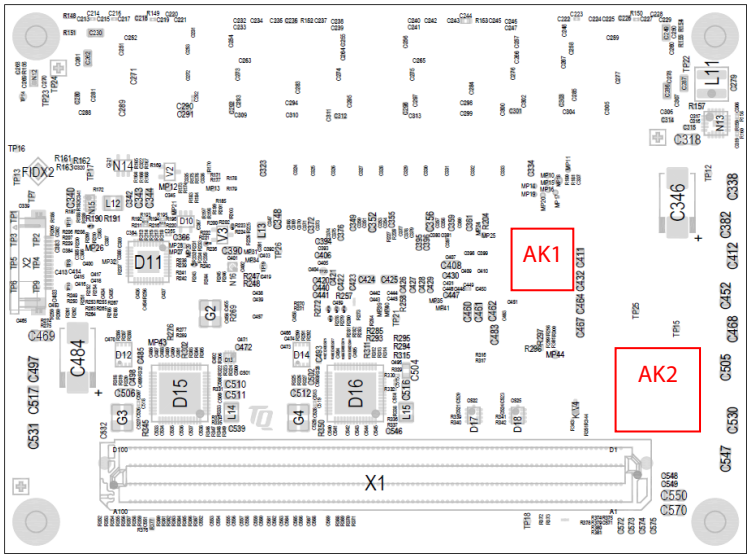

Figure 8: TQMxCU1-HPCM Component Placement Bottom

Table 17: Labels on TQMxCU1-HPCM

Label	Content
AK1	TQMxCU1-HPCM version and revision / MAC address
AK2	BIOS label

4.3 Heat Spreader

An aluminium heat spreader "TQMxCU1-HPCM-HSP" is available for the TQMxCU1-HPCM.
The TQMxCU1-HPCM can also be delivered with pre-mounted heat spreader (optional).
The provided heat spreader complies with the latest COM-HPC® Mini specification (10 mm ±0.2 mm, including PCB).

The following illustration shows the heat spreader (TQMxCU1-HPCM-HSP) for the TQMxCU1-HPCM.

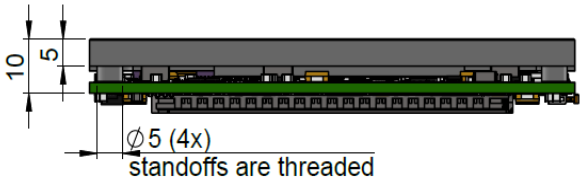

Figure 9: TQMxCU1-HPCM-HSP Heat Spreader

The White Paper "Heat Spreader Mounting Instruction" provides information how to mount the heat spreader.
Please contact TQ-Support for more details about 2D/3D STEP models.

4.4 Mechanical and Thermal Considerations

The TQMxCU1-HPCM is designed to operate within a wide range of thermal environments.
An important factor for each system integration is the thermal design. The heat spreader provides the thermal coupling to the TQMxCU1-HPCM. The heat spreader is thermally coupled to the processor and provides optimal heat transfer from the TQMxCU1-HPCM to the heat sink. The heat spreader itself is not an appropriate heat sink.
System designers can implement passive and active cooling systems using the thermal connection to the heat spreader.

Attention: Thermal Considerations	
	Do not operate the TQMxCU1-HPCM without properly attached heat spreader and heat sink!

If a special cooling solution is required, an extensive thermal design analysis and verification has to be performed.
TQ-Systems GmbH offers thermal analysis and simulation as a service.

4.5 Protection against External Effects

The TQMxCU1-HPCM itself is not protected against dust, external impact and contact (IP00).
Adequate protection has to be guaranteed by the surrounding system and carrier board.
Conformal coating can be offered for harsh environment applications.

5. SOFTWARE

5.1 System Resources

5.1.1 I2C0 Bus Devices

The TQMxCU1-HPCM provides a general-purpose I2C0 port via I²C controller in the TQ-flexiCFG block.
The following table shows the I2C0 address mapping for the COM-HPC® Mini I2C0 port.

Table 18: I²C Address Mapping COM-HPC® Mini I2C0 Port

8-bit Address	Function	Remark
0xA0	Module EEPROM	–
0xAE	Carrier board EEPROM	Embedded EEPROM configuration not supported

Make sure the address space of the carrier board I2C0 devices does not overlap the address space of the module devices.

5.1.2 SMBus

The TQMxCU1-HPCM provides a System Management Bus. No device is connected to the SMBus on the TQMxCU1-HPCM.

5.1.3 Memory Mapping

The TQMxCU1-HPCM supports the standard PC system memory and I/O memory map.

5.1.4 Interrupt Mapping

The TQMxCU1-HPCM supports the standard PC Interrupt routing.
The integrated legacy devices (COM1, COM2) can be configured via the BIOS to IRQ3 and IRQ4.

5.2 Operating Systems

5.2.1 Supported Operating Systems

The TQMxCU1-HPCM supports several Operating Systems:

- Microsoft® Windows® 10 (IoT) Enterprise (64-bit) LTSC 2021 or later
- Microsoft® Windows® 11 (IoT) Enterprise (64-bit)
- Linux Ubuntu (64-bit)

Other Operating Systems are supported on request.
Please visit TQ-Group (tab “Specifications”) or contact TQ-Support for further information about supported Operating Systems.

5.2.2 Driver Download

The TQMxCU1-HPCM is well supported by the Standard Operating Systems, which already include most of the drivers required.
It is recommended to use the latest Intel® drivers to optimize performance and make use of the full TQMxCU1-HPCM feature set.

The White Paper “Windows Driver Installation Instructions” provides information how to install the Windows driver.
Please visit TQ-Group or contact TQ-Support for further driver download assistance.

5.3 TQ-Systems Embedded Application Programming Interface (EAPI)

The TQ-Systems Embedded Application Programming Interface (EAPI) is a driver package to access and control hardware resources on all TQ-Systems COM-HPC® Mini modules. The TQ-Systems EAPI is compatible with the PICMG® specification.

5.4 Software Tools

Please visit Support TQ-Group or contact TQ-Support for further information about available software tools.

6. BIOS – MENU

The TQMxCU1-HPCM uses a 64-bit UEFI BIOS.
To access the InsydeH2O BIOS Front Page, the button <ESC> has to be pressed after System Power-Up during POST phase.
If the button is successfully pressed, you will get to the BIOS front page, which shows the main menu items.
Press <F1> for the Help Dialog.

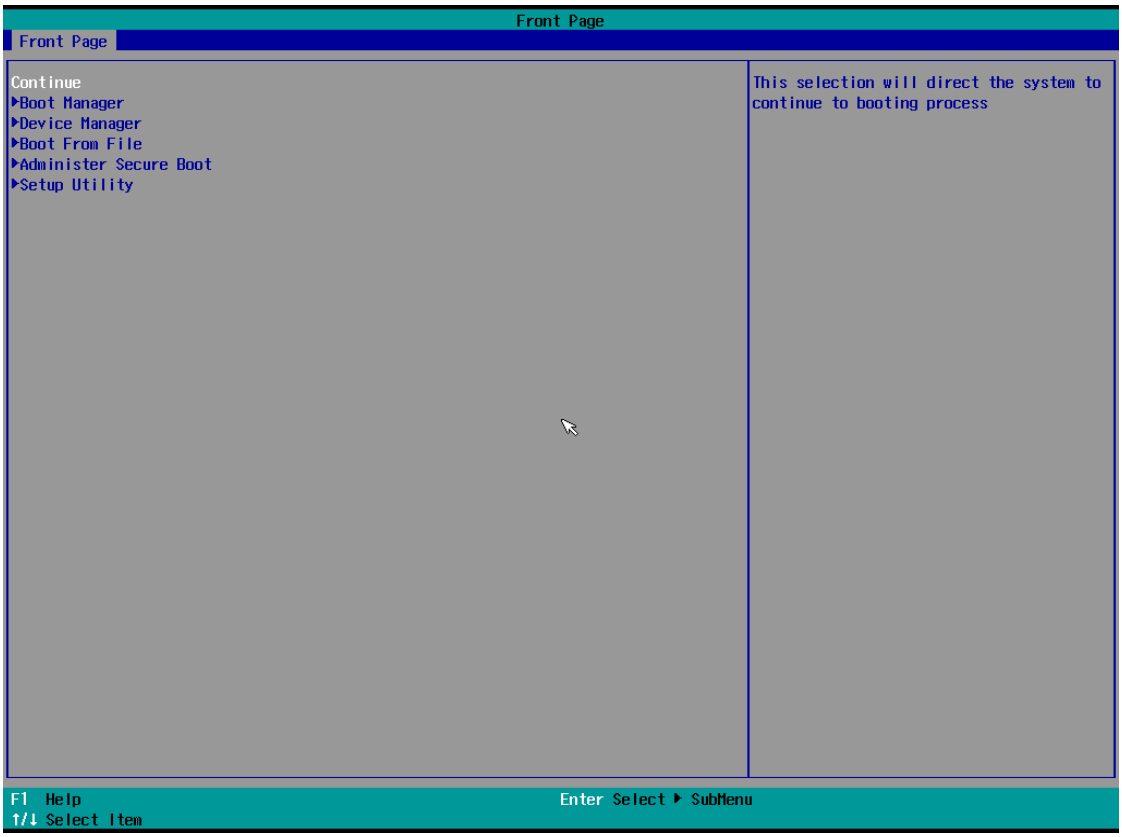

Figure 10: InsydeH2O BIOS Front Page

6.1 Continue

Continue boot process the same way if <ESC> was not pressed.

6.2 Boot Manager

Choose between possible boot options. One boot option will always be “Internal EFI Shell”.
You can go back to “Boot Manager” by entering the command “exit” and press <ENTER>.

6.3 Device Manager

6.3.1 Driver Health Manager

List all the driver health instances to manage.

6.3.2 Network Device List

Select the network device according the MAC address.

6.4 Boot from File

Boot from a specific mass storage device where a boot file is stored.

6.5 Administer Secure Boot

Enable and configure Secure Boot mode. This option can be also used to integrate PK, KEK, DB and DBx.

Note: Secure Boot	
	Only advanced users should use this option.

6.6 Setup Utility

A basic setup of the board can be done by Insyde Software Corp. “Insyde Setup Utility” stored inside an on-board SPI flash.
To get access to InsydeH2O Setup Utility the button <ESC> has to be pressed after System Power Up during POST phase.
After that, the sentence "ESC is pressed. Go to boot options" is displayed below the boot logo. Select "Setup Utility" on the splash screen that appears. The left frame of each menu page shows the option that can be configured, while the right frame shows the corresponding help.

Key:

↑ / ↓	Navigate between setup items.
← / →	Navigate between setup screens (Main, Advanced, Security, Power, Boot and Exit).
<F1>	Show general help screen (Key Legend).
<F5> / <F6>	Switch between different languages in the main screen. Change the value of the highlighted menu item in other screens.
<ENTER>	Press to show or change setup option listed for a certain menu or to show setup sub-menus.
<F9>	Press to load the default configuration (cannot be altered by the user). This option has to be confirmed and saved with <F10>. Leaving the InsydeH2O Setup Utility will discard all changes.
<F10>	Press to save any changes and exit setup utility by executing a restart.
<ESC>	Press to leave the current screen or sub-menu and discard all changes.

6.6.1 BIOS Main Screen

The Main screen shows details regarding the BIOS version, processor type, bus speed, memory configuration and further information. Three options can be configured.

Menu Item	Option	Description
Language	English / French / Korean / Chinese	Configures the language of the InsydeH2O Setup Utility
System Time	HH:MM:SS	Use to change the system time to the 24-hour format
System Date	MM:DD:YYYY	Use to change the system date

6.6.2 Advanced

Use the right cursor to get from the main menu item to the advanced menu item.

Menu Item	Option	Description
Boot Configuration	See submenu	Configures settings for Boot Phase
USB Configuration	See submenu	Configure the USB support
Chipset Configuration	See submenu	Advanced Chipset Configuration options
ACPI Table/Features Control	See submenu	Configures ACPI Tables/Features setting
CPU Configuration	See submenu	CPU Configuration
Power & Performance	See submenu	Power & Performance
Memory Configuration	See submenu	Memory Configuration Parameters
System Agent (SA) Configuration	See submenu	System Agen (SA) Parameters
PCIE Configuration	See submenu	PCIE Parameters
PCH-IO Configuration	See submenu	PCH Parameters
PCH-FW Configuration	See submenu	Configure Management Engine Technology Parameters
Platform Settings	See submenu	Platform related settings
ACPI D3Cold Settings	See submenu	ACPI D3Cold related settings
SIO TQMx86	See submenu	Configure CPLD UARTs, TQ Board specific configuration and LVDS
H20Uve Configuration	See submenu	Show H20Uve Configuration
Console Redirection Configuration	See submenu	Configure Console Redirection settings

6.6.2.1 Boot Configuration

Setup Utility ⇨ Advanced ⇨ Boot Configuration

Menu Item	Option	Description
Numlock	On / Off	Allows to choose whether NumLock key at system boot must be turned On or Off

6.6.2.2 USB Configuration

Setup Utility ⇨ Advanced ⇨ USB Configuration

Menu Item	Option	Description
USB BIOS Support	Enabled / Disabled	USB keyboard/mouse/storage support under UEFI environment.
USB Legacy SMI bit Clean	Enabled / Disabled	Clean USB Legacy SMI bit for xHCI and EHCI

6.6.2.3 Chipset Configuration

Setup Utility ⇨ Advanced ⇨ Chipset Configuration

Menu Item	Option	Description
Platform Trust Technology	Enabled / Disabled	Enable/Disable Platform Trust Technology. Disable this option to use discrete TPM (dTPM).

6.6.2.4 ACPI Table/Features Control

Setup Utility ⇨ Advanced ⇨ ACPI Table/Features Control

Menu Item	Option	Description
ACPI Settings	See submenu	System ACPI Parameters
FACP – RTC S4 Wakeup	Enabled / Disabled	Value only for ACPI. Enable/Disable for S4 Wakeup from RTC.
APIC – IO APIC Mode	Enabled / Disabled	This item is valid only for WIN2k and WINXP. Also, a fresh install of the OS must occur when APIC Mode is desired. Test the IO ACPI by setting item to Enable. The APIC Table will then be pointed to by the RSDT, the Local APIC will be initialized, and the proper enable bits will be set in ICH4M.

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ ACPI Settings

Menu Item	Option	Description
Enable ACPI Auto Configuration	[ ] / [X]	Enables or disables BIOS ACPI auto configuration
Enable Hibernation	[ ] / [X]	Enables or disables system ability to hibernate (OS/S4 Sleep State). This option may not be effective with some OSs.
PTID Support	[ ] / [X]	PTID support will be loaded if enabled.
PECI Access Method	Direct I/O / ACPI	PECI Access Method is Direct I/O or ACPI
Native PCIE Enable	Enabled / Disabled	Enables or disables Native PCIE
Native ASPM	Auto / Enabled / Disabled	Enabled – OS controlled ASPM Disabled – BIOS controlled ASPM
BDAT ACPI Table Support	Enabled / Disabled	Enables support for the BDAT ACPI table
Safe Setting	Enabled / Disabled	This is master token to control safe settings. It will be useful with XmlCli
ACPI Debug	Enabled / Disabled	Open a memory buffer for storing debug strings. Reenter SETUP after enabling to see the buffer address. Use method ADBG to write strings to buffer.
D3 Setting for Storage	Enabled / Disabled	RTD3 support for Storage. PCIE storage PEP constraint needs to be set as D0/F1 (Intel Advanced -> ACPI Settings PEP PCIe Storage) when this setup is disabled/D3Hot.
Low Power S0 Idle Capability	Enabled / Disabled	This variable determines if we enable ACPI Lower Power S0 Idle Capability (Mutually exclusive with Smart connect). While this is enable, it also disable 8254 timer for SLP_S0 support.
PUIS Enable	Enabled / Disabled	Enable/Disable Power-Up in Standby (PUIS) feature set allows to be powered-up into the Standby power current at power-up and to allow the host to sequence the spin-up of devices.
SSDT table from file	Enabled / Disabled	SSDT table from file.
PCI Delay Optimization	Enabled / Disabled	Experimental ACPI additions for FW latency optimizations.
MSI enabled	Enabled / Disabled	When disabled, MSI support is disabled in FADT.
PCIe delay between_OFF_ON	[Yes] / [No]	Delay will be applied to all PCIe devices between OFF and ON methods to make sure minimum delay is passed before calling the ON sequence except WWAN, (Range 50ms to 500ms)

6.6.2.5 CPU Configuration

Setup Utility ⇨ Advanced ⇨ CPU Configuration

Menu Item	Options	Description
Efficient-core Information	See submenu	Displays the E-core Information
Performance-core	See submenu	Displays the P-core Information
CPU Flex Ratio Override	Enabled / Disabled	Enable7Disable CPU Flex Ratio Programming
Intel (VMX) Virtualization Technology	Enabled / Disabled	When enabled, a VMM can utilize the additional hardware capabilities provide by Vanderpool Technology.
AVX	Enabled / Disabled	Enable/Disable the AVX and AVX2 Instructions
Active Performance-cores	All / 1	Number of P-cores to enable in each processor package. Note: Number of Cores and E-Cores are looked at together. When both are (0, 0), Pcode will enable all cores.
Active Efficient-cores	All / 0 / 1 / 2 / 3 / 4 / 5 / 6 / 7	Number of E-cores to enable in each processor package. Note: Number of Cores and E-Cores are looked at together. When both are (0, 0), Pcode will enable all cores.
Active SOC-North Efficient-cores	All / 1 / 0	Number of SOC-North Efficient-cores to enable in SOC North.
Hyper-Threading	Enabled / Disabled	Enable or Disable Hyper-Threading Technology.
BIST	Enabled / Disabled	Enable/Disable BIST (Built-In Self Test) on reset
AP threads Idle Manner	HALT Loop / MWAIT Loop / RUN Loop	AP threads Idle Manner for waiting signal to run
AES	Enabled / Disabled	Enable/Disable AES (Advanced Encryption Standard)
MachineCheck	Enabled / Disabled	Enable/Disable Machine Check
MonitorMWait	Enabled / Disabled	Enable/Disable MonitorMWait, if Disable MonitorMWait, the AP threads Idle Manner should not set in MWait Loop
Intel Trusted Execution Technology	Enabled / Disabled	Enable Intel Trusted Execution Technology
Alias Check Request	Enabled / Disabled	Enable or Disable Alias Check Request.
DPR Memory Size (MB)	[X]	Define DPR Memory Size in MB.
Reset AUX Content	Yes / No	Reset AUX Content
X2APIC Enable	Enabled / Disabled	Enable/Disable X2APIC Operating Mode. When this option is configured as “Enabled”, “VT-d” option must be “Enabled” and “X2APIC Opt Out” option must be “Disabled” as well. This option will be grayed out when “VT-d” option is configured as “Disabled”.

6.6.2.6 Power & Performance

Setup Utility ⇨ Advanced ⇨ Power & Performance

Menu Item	Options	Description
CPU – Power Management Control	See submenu	CPU – Power Management Control Options
GT/Media – Power Management Control	See submenu	GT – Power Management Control Options
Overclocking Lock	Enabled / Disabled	Enable/Disable Overclocking Lock.
Intel ® Speed Shift Technology Interrupt Control	Enabled / Disabled	Enable/Disable Intel ® Speed Shift Technology Interrupts

Setup Utility ⇨ Advanced ⇨ Power & Performance ⇨ CPU – Power Management Control

Menu Item	Options	Description
Boot Max Frequency	Enabled / Disabled	Enable/Disable Boot Maximum Frequency in CPU strap.
Boot performance mode	Max Battery / Max Non-Turbo Performance / Turbo Performance	Select the performance state that the BIOS will set starting from reset vector.
Intel® SpeedStep™	Enabled / Disabled	Allows more than two frequency ranges to be supported.
Race To Halt (RTH)	Enabled / Disabled	Enable or Disable Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power.
Intel® Speed Shift Technology	Enabled / Disabled	Enable or Disable Intel® Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.
Per Core P State OS control mode	Enabled / Disabled	Enable/Disable Per Core P state OS control mode. Disabling will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core requests.
HwP Autonomous Per Core P State	Enabled / Disabled	Disable Autonomous PCPS (Bit 30 = 1, command 0x11) Autonomous will request the same value for all cores all the time. Enable PCPS (default Bit 30 = 0, command 0x11)
HwP Autonomous EPP Grouping	Enabled / Disabled	Enable EPP grouping (default Bit 29 = 0, command 0x11) Autonomous will request the same values for all cores with same ePP. Disable EPP grouping (Bit 29 = 1, command 0x11) autonomous will not necessarily request same values for all cores with same EPP.
HwP Lock	Enabled / Disabled	Enable/Disable HWP Lock support in Misc Power Management MSR.
Turbo Mode	Enabled / Disabled	Enable or Disable processor Turbo Mode (requires Intel® Speed Step or Intel® Speed Shift to be available and enabled).
View/Configure Turbo Options	See submenu	Configure Turbo Options.
Config TDP Configurations	See submenu	Configure TDP Options.
CPU VR Settings	See submenu	Configure CPU VR Settings.
Platform PL1 Enable	Enabled / Disabled	Enable/Disable Platform Power Limit 1 programming. If this option is enabled. It activates the PL1 value to be used by the processor to limit the average power of given time window.
Platform PL2 Enable	Enabled / Disabled	Enable/Disable Platform Power Limit 2 programming. If this option is disabled, BIOS will program the default values for Platform Power Limit 2.
Power Limit 4 Override	Enabled / Disabled	Enable/Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Power Limit 4.
Power Limit 4 Boost	[Yes] / [No]	Configure Power Limit 4 Boost in Watts. The value 0 mean disable.
C states	Enabled / Disabled	Enable or Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
Enhanced C-states	Enabled / Disabled	Enable/Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State.
C-State Auto Demotion	Disabled / C1	Configure C-State Auto Demotion. This option will be hidden if C states is Disabled.
C-State Un-demotion	Disabled / C1	Configure C-State Un-demotion. This option will be hidden if C states is Disabled.
Package C-State Demotion	Enabled / Disabled	Package C-State Demotion. This option will be hidden if C states is Disabled.
Package C-State Un-demotion	Enabled / Disabled	Package C-State Un-demotion. This option will be hidden if C states is Disabled.
CState Pre-Wake	Enabled / Disabled	Disabled: Sets bit 30 of Power_CTL MSR (0x1FC) to 1 to disable the CState Pre-Wake. This option will be hidden if C states is Disabled.
IO MWAIT Redirection	Enabled / Disabled	When set, will map IO_read intstructions sent to IO registers

Menu Item	Options	Description
		PMG_IO_BASE_ADDRBASE + offset to MWAIT(offset)
Package C State Limit	C0/C1 / C2 / C3 / C6 / C7 / C7S / C8 / C9 / C10 / CPU Default / Auto	Maximum Package C State Limit Setting. CPU Default: Leaves to Factory default value. Auto: Initializes to deepest available Package C State Limit. This option will be hidden if C states is Disabled.
Thermal Monitor	Enabled / Disabled	Enable or Disable Thermal Monitor. This option will be hidden if C states is Disabled.
Interrupt Redirection Mode Selection	Fixed Priority / Round robin / Hash Vector / No Change	Interrupt Redirection Mode Select for Logical Interrupts.
Timed MWAIT	Enabled / Disabled	Enable/Disable Timed MWAIT Support.
Power Limit 3 Settings	See submenu	Power Limit 3 Settings
CPU Lock Configuration	See submenu	CPU Lock Configuration

Setup Utility ⇨ Advanced ⇨ Power & Performance ⇨ CPU – Power Management Control ⇨ View/Configure Turbo Options

Menu Item	Options	Description
Turbo Ratio Limit Options	See submenu	View/Configure Turbo Ratio Limit Options.
Energy Efficient P-state	Enabled / Disabled	Enable/Disable Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function will read 0 indication no support for Energy Efficient policy setting. When set to 1 will enable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function will read 1 indication Energy Efficient policy setting is supported.
Package Power Limit MSR Lock	Enabled / Disabled	Enable/Disable locking of Package Power Limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register.
Energy Efficient Turbo	Enabled / Disabled	Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overlocking situations where turbo frequency must remain constant. Otherwise, leave enabled.

Setup Utility ⇨ Advanced ⇨ Power & Performance ⇨ CPU – Power Management Control ⇨ View/Configure Turbo Options ⇨ Turbo Ratio Limit Options

Menu Item	Options	Description
P-core Turbo Ratio Limit CoreX	[X]	Performance-core Turbo Ratio Limit CoreX defines the core range, the turbo ratio is defined in Turbo Ratio Limit RatioX. If value is zero, this entry is ignored.
P-core Turbo Ratio Limit RatioX (TRLR)	[X]	Performance-core Turbo Ratio Limit RatioX (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode). This Turbo Ratio Limit RatioX must be greater than or equal all other ratio values. If this value is invalid, then set all other active cores to minimum. Otherwise, align the Ratio Limit to 0. Please check each active cores
E-core Turbo Ratio Limit CoreCountX	[X]	Efficient-core Turbo Ratio Limit CoreCountX defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit RatioX. If value is zero, this entry is ignored.
E-core Turbo Ratio Limit RatioX	[X]	Efficient-core Turbo Ratio Limit RatioX defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit CoreCountX.

Setup Utility ⇨ Advanced ⇨ Power & Performance ⇨ CPU – Power Management Control ⇨ Config TDP Configurations

Menu Item	Options	Description
Enable Configurable TDP	Applies to non-cTDP / Applies to cTDP	Applies TDP initialization settings basen on non-cTDP or cTDP. Default is 1: Applies to cTDP; if 0 then applies to non cTDP and BIOS will bypass cTDP initialization flow.
Configurable TDP Boot Mode	Nominal / Level 1 / Level 2 / Deactivate	Configurable Processor Base Power (cTDP) Mode as Nominal / Level 1 / Level 2 / Deactivate TDP selection. Deactivate option will set MSR to Nominal and MMIO to Zero.
Configurable TDP Lock	Enabled / Disabled	Configurable TDP Mode Lock sets the Lock bits on TURBO_ACTIVATION_RATIO and CONFIG_TDP_CONTROL. Note: When CTDP Lock is enabled Custom ConfigTDP Count will be forced to 1 and Custom ConfigTDP Boot index will be forced to 0.
CTDP BIOS control	Enabled / Disabled	Enables cTDP (Assured Power) control via runtime ACPI BIOS methods. This “BIOS only” feature does not require EC or driver support.
ConfigTDP Nominal	Ratio:13 TAR:12 PL1:15.0W	cTDP (Assured Power) Nominal Ratio and Processor Base Power (TDP) from MSR
Power Limit 1	[X]	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overlocking SKU: Value must be between Max and Min Power Limits. Other SKUs: This value must be between Min Power Limit and Processor Base Power (TDP) Limit.
Power Limit 2	[X]	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window	0 – 128	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines time window which Processor Base Power (TDP) value should be maintained.
ConfigTDP Turbo Activation Ratio	[X]	Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don`t use custom value.
ConfigTDP Level1	Ratio:10 TAR:9 PL1:12.0W	cTDP (Assured Power) Level1 Ratio and Processor Base Power (TDP) from MSR
Power Limit 1	[X]	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overlocking SKU: Value must be between Max and Min Power Limits. Other SKUs: This value must be between Min Power Limit and Processor Base Power (TDP) Limit.
Power Limit 2	[X]	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window	0 – 128	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines time window which Processor Base Power (TDP) value should be maintained.
ConfigTDP Turbo Activation Ratio	[X]	Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don`t use custom value.
ConfigTDP Level2	Ratio:27 TAR:26 PL1:28.0W	cTDP (Assured Power) Level2 Ratio and Processor Base Power (TDP) from MSR
Power Limit 1	[X]	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overlocking SKU: Value must be between Max and Min Power Limits. Other SKUs: This value must be between Min Power Limit and Processor Base Power (TDP) Limit.
Power Limit 2	[X]	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W

Menu Item	Options	Description
		when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window	0 – 128	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines time window which Processor Base Power (TDP) value should be maintained.
ConfigTDP Turbo Activation Ratio	[X]	Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don`t use custom value.

Setup Utility ⇨ Advanced ⇨ Power & Performance ⇨ CPU – Power Management Control ⇨ CPU VR Settings

Menu Item	Options	Description
PSYS Slope	[X]	PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0=Auto. Uses BIOS VR mailbox command 0x9.
PSYS Offset	[X]	PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. PSYS uses BIOS VR mailbox command 0x4.
PSYS Prefix	+ / -	Sets the offset value as positive or negative.
PSYS PMax Power	[X]	PSYS PMax power, defined in 1/8 Watt or Percent increments. For Watts, Range is 0-8191 (ex. for 125W, enter 1000). For ATX12V0 Percent, Range is 0-1600 (ex. for 200%, enter 1600). Uses BIOS VR mailbox command 0xB.
Vsys/Psys Critical	Disabled / Psys Critical / Vsys Critical	Vsys/Psys Critical Enable or disable
Assertion Deglitch Mantissa	[X]	Assertion Deglitch Mantissa 0x4F [7-3]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
Assertion Deglitch Exponent	[X]	Assertion Deglitch Exponent 0x4F [3-0]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
De assertion Deglitch Mantissa	[X]	De Assertion Deglitch Mantissa 0x49 [7-3]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
De assertion Deglitch Exponent	[X]	De Assertion Deglitch Exponent 0x49 [3-0]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
SVID Stabilization Delay	[X]	Configure SVID Stabilization Delay (in us) being used for the FVM feature when it is enabled. Note that this delay applies to all SVID domains equally (no unique values possible for IA/GT/SA).
Acoustic Noise Settings	See submenu	Configure Acoustic Noise Settings for Core, GT and SA domains
Efficiency/Performance VR Settings	See submenu	Efficiency/Performance VR Settings
GT VR Settings	See submenu	GT VR Settings
SA VR Settings	See submenu	SA VR Settings
RFI Settings	See submenu	RFI Settings

Setup Utility ⇨ Advanced ⇨ Power & Performance ⇨ CPU – Power Management Control ⇨ CPU VR Settings ⇨ Acoustic Noise Settings

Menu Item	Options	Description
Acoustic Noise Mitigation	Enabled / Disabled	Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state
Pre Wake Time	[X]	Set the maximum Pre Wake randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Perodicity Alteration (DPA) tuning.
Ramp Up Time	[X]	Set the maximum Ramp Up randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Perodicity Alteration (DPA) tuning.
Ramp Down Time	[X]	Set the maximum Ramp Down randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Perodicity Alteration (DPA) tuning.
Disable Fast PKG C State Ramp for Core Domain	FALSE / TRUE	This option needs to be configured to reduce acoustic noise during deeper C states. False: Don`t disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state
Slow Slew Rate for Core Domain	Fast/2 / Fast/4 / Fast/8 / Fast/16	Set VR Core Slow Slew Rate for Deep Package C Sate ramp time; Slow slew rate equals to Fast divided be number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise
Disable Fast PKG C State Ramp for GT Domain	FALSE / TRUE	This option needs to be configured to reduce acoustic noise during deeper C states. False: Don`t disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state
Slow Slew Rate for GT Domain	Fast/2 / Fast/4 / Fast/8	Set VR GT Slow Slew Rate for Deep Package C Sate ramp time; Slow slew rate equals to Fast divided be number, the number is 2, 4, 8 to slow down the slew rate to help minimize acoustic noise; divide by 16 is disabled
Disable Fast PKG C State Ramp for SA Domain	FALSE / TRUE	This option needs to be configured to reduce acoustic noise during deeper C states. False: Don`t disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state

Setup Utility ⇨ Advanced ⇨ Power & Performance ⇨ CPU – Power Management Control ⇨ CPU VR Settings ⇨ RFI Settings

Menu Item	Options	Description
Global DLVR RFI Mitigation Control	Enabled / Disabled	Enable/Disable Global DLVR RFI Mitigation Control
DLVR SSC Value	[X]	DLVR SSC in percentage with multiple of 0.25%. 0 = 0%, 31 = 7.75%.
DLVR RFI Frequency	[X]	DLVR RFI Frequency in MHz.

Setup Utility ⇨ Advanced ⇨ Power & Performance ⇨ CPU – Power Management Control ⇨ Power Limit 3 Settings

Menu Item	Options	Description
Power Limit 3 Override	Enabled / Disabled	Enable/Disable Power Limit 3 override. If this option is disabled, BIOS will leave the hardware default values for Power Limit 3 and Power Limit 3 Time Window.
Power Limit 3	[X]	Power Limit 3 in Milli Watts/Percent. BIOS will round to the nearest 1/8W when programming. For example, if 12.50W, enter 12500, if 12%, enter 12000, if 50%, enter 50000. XE SKU: Any value can be programmed. Overlocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and Processor Base Power (TDP) Limit. If when value is 0, BIOOS leaves the hardware default value
Power Limit 3 Time Window	[X]	Power Limit 3 Time Window value in Milli seconds. The value may vary

Menu Item	Options	Description
		from 3 to 64(max). Indicates the time window over which Power Limit 3 value should be maintained. If the value is 0, BIOS leaves the hardware default value
Power Limit 3 Duty Cycle	[X]	Specify the duty cycle in percentage that the CPU is required to maintain over the configured time window. Range is 0-100.
Response Mode	Gradual Power Reduction / Aggressive Power Reduction	Use Response Mode to adjust Psys_PL3 power reduction behaviour. Battery-enabled systems use Gradual Power Reduction.
Power Limit 3 Lock	Enabled / Disabled	Power Limit 3 Lock. When enabled PL3 configurations are locked during OS. When disabled PL3 configuration can be changed during OS.

Setup Utility ⇨ Advanced ⇨ Power & Performance ⇨ CPU – Power Management Control ⇨ CPU Lock Configuration

Menu Item	Options	Description
CFG Lock	Enabled / Disabled	Configure MSR to CFG Lock bit

Setup Utility ⇨ Advanced ⇨ Power & Performance ⇨ GT/Media – Power Management Control

Menu Item	Options	Description
RC6 (Render Standby)	Enabled / Disabled	Check to enable render standby support.
MC6(Media Standby)	Enabled / Disabled	Check to enable Media standby support.
Maximum GT frequency	Default Max Frequency / 100Mhz – 1200Mhz	Maximum GT frequency limited by the user. Choose between 2400MHz (RPN) and 5550MHz (RP0). Value beyond the range will be clipped to min/max supported by SKU
Disable Turbo GT frequency	Enabled / Disabled	Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited.

6.6.2.7 Memory Configuration

Setup Utility ⇨ Advanced ⇨ Memory Configuration

Menu Item	Option	Description
MRC Safe Mode Override	[X]	Bit mask to enable the use of the input safe mode values. When a bit is set, the corresponding safe mode input field value will be used instead of the pre-defined MRC safe mode configuration. The definitions are: [0] Enable DdrSafeMode override, [1] Enable McSafeMode override, [2] Enable MrcSafeMode override, [3] Enable Training Algorithm (Training Enables) safe mode override, [4] Enable SaGv safe mode override
Memory Test on Warm Boot	Enabled / Disabled	Enable Or Disable Base Memory Test Run on Warm Boot
Maximum Memory Frequency	Auto / 1067 – 12800	Maximum Memory Frequency Selections in Mhz.
SAGV	Enabled / Disabled	System Agent Geyserville. Disabled or Enabled.
SA GC Mask	Enable Points: 1st and 2nd / Enable Points: 1st, 2nd, and 3rd / Enable All Points: 1st, 2nd, 3rd, and 4th	System Agent Geyserville. Set the BIT(s) for which points to use in frequency switching.
First Point Frequency	[X]	Specify the frequency for the given point. 0 – MRC auto, Else a specific frequency as an integer: 1333
First Point Gear	Auto / Gear2 / Gear4	Gear ratio for this SAGV point.
Second Point Frequency	[X]	Specify the frequency for the given point. 0 – MRC auto, Else a specific frequency as an integer: 1333

Menu Item	Option	Description
Second Point Gear	Auto / Gear2 / Gear4	Gear ratio for this SAGV point.
Third Point Frequency	[X]	Specify the frequency for the given point. 0 – MRC auto, Else a specific frequency as an integer: 1333
Third Point Gear	Auto / Gear2 / Gear4	Gear ratio for this SAGV point.
Fourth Point Frequency	[X]	Specify the frequency for the given point. 0 – MRC auto, Else a specific frequency as an integer: 1333
Fourth Point Gear	Auto / Gear2 / Gear4	Gear ratio for this SAGV point.
Row Hammer Mode	Disabled / RFM / pTRR	Row Hammer Prevention Mode. RFM will fall back to pTRR if not available.
Refresh Watermarks	Low / High	Sets Refresh Panic Watermark and Refresh High-Priority Watermark to HIGH or LOW values
Extended Bank Hashing	Enabled / Disabled	Enable/disable Extended Bank Hashing.
Per Bank Refresh	Enabled / Disabled	Enables and Disables the per bank refresh. This only impacts memory technologies that support PBR: LPDDR3, LPDDR4.
Memory Scrambler	Enabled / Disabled	Enable/Disable Memory Scrambler support.
Force ColdReset	Enabled / Disabled	Force ColdReset OR Choose MrcColdBoot mode, when Coldboot is required during MRC execution. Note: If ME 5.0MB is present, ForceColdReset is required!
In-Band ECC Support	Enabled / Disabled	Enable/Disable In-Band ECC. Will be enabled if memory has symmetric configuration.
In-Band ECC Operation Mode	0 / 1 / 2	0: Functional Mode protects requests based on the address range, 1: Makes all requests non protected and ignore range checks, 2: Makes all requests protected and ignore range checks
In-Band ECC Error Injection Control	No Error Injection / Inject Correctable Error Address match / Inject Correctable Error on insertion counter / Inject Uncorrectable Error Address match / Inject Uncorrectable Error on insertion counter	Enables IBECC Error Injection

6.6.2.8 System Agent (SA) Configuration

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration

Menu Item	Options	Description
Graphics Configuration	See submenu	Graphic Configuration
TCSS setup menu	See submenu	TCSS Configuration settings
VMD setup menu	See submenu	VMD Configuration settings
VT-d setup menu	See submenu	VT-d Configuration settings
GNA Device (B0:D8:F0)	Enabled / Disabled	Enable/Disable SA GNA Device.
CRID Support	Enabled / Disabled	Enable/Disable SA CRID and TCSS CRID control for Intel SIPP
Above 4GB MMIO BIOS assignment	Enabled / Disabled	Enable/Disable above 4GB MemoryMappedIO BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB.
IPU Device (B0:D5:F0)	Enabled / Disabled	Enable/Disable SA IPU Device. This option will be grayed out when IPU is fussed off from silicon.
NPU Device (B0:D11:F0)	Enabled / Disabled	Enable/Disable NPU (Neural Processing Unit) Device.
MIPI Camera Configuration	See submenu	MIPI Camera Configuration

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration ⇨ Graphics Configuration

Menu Item	Option	Description
Skip Scanning of External Gfx Card	Enabled / Disabled	If enabled, it will not scan for External Gfx Card on PCIE Ports.
Primary Display	Auto / IGFX / HG	Select AUTO set IGD to be Primary Display if no external Graphics connected otherwise external Graphics Device detected on first PCIe port will be Primary Display or Select IGFX for IGD to be Primary Display Or Select HG for Hybrid Gfx.
Internal Graphics	Auto / Enabled / Disabled	Keep IGFX enabled based on the setup options.
Intel Graphics Pei Display Peim	Enabled / Disabled	Enable/Disable Pei (Early) Display
VDD Enable	Enabled / Disabled	Enable/Disable forcing of VDD in the BIOS
Configure GT for use	Enabled / Disabled	Enable/Disable GT configuration in BIOS
Configure Media for use	Enabled / Disabled	Enable/Disable Media configuration in BIOS
GT RC1p Support	Enabled / Disabled	Enable/Disable RC1p support. If GT RC1p is enabled, send a RC1p frequency request to PMA if other conditions being met
Media RC1p Support	Enabled / Disabled	Enable/Disable RC1p support. If Media RC1p is enabled, send a RC1p frequency request to PMA if other conditions being met
PAVP Enable	Enabled / Disabled	Enable/Disable PAVP
V-by-One(iTE6807) Enable	Enabled / Disabled	Enable/Disable V-by-One(iTE6807)
Bypass VBT Update	Enabled / Disabled	Enable/Disable bypass VBT update
IUER Button Enable	Enabled / Disabled	Enable/Disable IUER Button Functionality

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration ⇨ TCSS setup menu

Menu Item	Option	Description
TCSS xHCI Support	Enabled / Disabled	Enable / Disable TCSS xHCI.
TCSS USB Configuration	See submenu	SA TCSS USB Configuration settings
I TBT PCIE0 Root Port	Enabled / Disabled	Enable/Disable I TBT PCIE ROOT
I TBT PCIE1 Root Port	Enabled / Disabled	Enable/Disable I TBT PCIE ROOT
I TBT PCIE2 Root Port	Enabled / Disabled	Enable/Disable I TBT PCIE ROOT
I TBT PCIE3 Root Port	Enabled / Disabled	Enable/Disable I TBT PCIE ROOT
I TBT DMA0	Enabled / Disabled	Enable/Disable I TBT DMA0
I TBT DMA1	Enabled / Disabled	Enable/Disable I TBT DMA1
VCCST status of IOM	Enabled / Disabled	Enables/Disables VCCST. Enable: Sends VCCST ON message or EC or PMC Disable: Sends VCCST OFF message to EC or PMC
D3 Cold Enable/Disable	Enabled / Disabled	Enables/Disables D3 Cold. Enable: D3 cold support for IOM is enabled Disable: D3 cold support for IOM is Disabled
D3 Hot Enable/Disable	Enabled / Disabled	Enables/Disables D3 Hot. Enable: D3 Hot support for IOM is enabled Disable: D3 Hot support for IOM is Disabled
Tc C-State Limit	Disable / 1 / 2 / 4 / 5 / 6 / 7 / 10	BIOS mailbox to limit deepest TCx state
PCI Express Root Port 3	See submenu	PCI Express Root Port 3 Settings.

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration ⇨ TCSS setup menu ⇨ TCSS USB Configuration

Menu Item	Option	Description
USB CONNECT OVERRIDE	Enabled / Disabled	Option will allow VCCSTTPC to turn off even when there is a connection for a USB3 port.
TCSS xDCI Support	Enabled / Disabled	Enable/Disable TCSS xDCI

Menu Item	Option	Description
TCSS CPU USB PD0 Programming	Enabled / Disabled	Select “Enabled” if Port Disable Override functionally is used.
TCSS CPU USB Port Disable Override	Disable / Select Per-Pin	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.
TCSS CPU USB SS Physical Connector #0	Enabled / Disabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
TCSS CPU USB SS Physical Connector #1	Enabled / Disabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
TCSS CPU USB SS Physical Connector #2	Enabled / Disabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
TCSS CPU USB SS Physical Connector #3	Enabled / Disabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration ⇨ TCSS setup menu ⇨ PCI Express Root Port 3

Menu Item	Option	Description
PTM	Enabled / Disabled	Enable/Disable Precision Time Measurement
LTR	Enabled / Disabled	PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Enabled / Disabled	Snoop Latency Override for SA PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Snoop Latency Value	[X]	LTR Snoop Latency value of SA PCIE
Snoop Latency Multiplier	1 ns / 32 ns / 1024 ns / 32768 ns / 1048576 ns / 33554432 ns	LTR Snoop Latency Multiplier of SA PCIE
Non Snoop Latency Override	Enabled / Disabled	Non Snoop Latency Override for SA PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Value	[X]	LTR Non Snoop Latency value of PCH PCIE
Non Snoop Latency Multiplier	1 ns / 32 ns / 1024 ns / 32768 ns / 1048576 ns / 33554432 ns	LTR Non Snoop Latency Multiplier of SA PCIE
Force LTR Override	Enabled / Disabled	Force LTR Override for I TBT PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
LTR Lock	Enabled / Disabled	PCIE LTR Configuration Lock

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration ⇨ VMD setup menu

Menu Item	Option	Description
Enable VMD Controller	Enabled / Disabled	Enable/Disable to VMD Controller
Enable VMD Global Mapping	Enabled / Disabled	Enable/Disable to VMD Global Mapping.
Map RP BDF 0/6/2 Under VMD	Enabled / Disabled	Map/UnMap this Root Port to VMD
Raid 0	Enabled / Disabled	Enable/Disable RAID0 support.
Raid 1	Enabled / Disabled	Enable/Disable RAID1 support.
Raid 5	Enabled / Disabled	Enable/Disable RAID5 support.

Menu Item	Option	Description
Raid 10	Enabled / Disabled	Enable/Disable RAID10 support.
Intel Rapid Recovery Technology	Enabled / Disabled	Enable/Disable Intel Rapid Recovery Technology.
RRT volumes can span internal and eSATA drives	Enabled / Disabled	Enable/Disable RRT volumes can span internal and eSATA drivers.
Intel® Optane™ Memory	Enabled / Disabled	Enable/Disable System Acceleration with Intel® Optane™ Memory feature.
ZP0DD	Enabled / Disabled	Enable/Disable ZP0DD. The option is only needed to be enabled when ZP0DD is connected in VMD mode

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration ⇨ VT-d setup menu

Menu Item	Option	Description
VT-d	Supported	Check to enable VT-d function on MCH. This option will be grayed out when “X2APIC Enable” option is configured as “Enabled”.
Pre-boot DMA Protection	Enabled / Disabled	Enable DMA Protection in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)
DMA Control Guarantee	Enabled / Disabled	Enable/Disable DMA_CONTROLL_GUARANTEE bit

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration ⇨ MIPI Camera Configuration

Menu Item	Option	Description
CVF/CVS Support	Enable(USB Bridge) / Disabled	Disable/Enable CVF/CVS
Control Logic 1	Enabled / Disabled	Control Logic 1
Control Logic 2	Enabled / Disabled	Control Logic 2
Control Logic 3	Enabled / Disabled	Control Logic 3
Control Logic 4	Enabled / Disabled	Control Logic 4
Camera1	Enabled / Disabled	Camera1
Camera2	Enabled / Disabled	Camera2
Camera3	Enabled / Disabled	Camera3
Camera4	Enabled / Disabled	Camera4

6.6.2.9 PCIE Configuration

Setup Utility ⇨ Advanced ⇨ PCIE Configuration

Menu Item	Options	Description
Port8xh Decode	Enabled / Disabled	PCI Expres Port8xh Decode Enable/Disable.
Compliance Test Mode	Enabled / Disabled	Enable when using Compliance Load Board
PCIE Resizable BAR Support	Auto / Enabled / Disabled	Enable/Disable PCIE Resizable BAR Support
PCI Express Root Port PXPX	See submenu	PCI Express Root Port Settings. PXPA = COM-HPC PCIe Ports 4-7 PXPB = COM-HPC PCIe Ports 0-3 PXPC = OnBoard Lan0 PXPD = COM-HPC PCIe Ports 8-11 (1x4) PXPE = COM-HPC PCIe Ports 12-15 (1x4)

Setup Utility ⇨ Advanced ⇨ PCIE Configuration ⇨ PCIE Express Root Port X

Menu Item	Options	Description
PCI Express Root Port x	Enabled / Disabled	Control the PCI Express root port.
Connection Type	Built-in / Slot	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
ASPM	Disabled / L0s / L1 / L0sL1 / Auto	PCI Express Active State Power Management settings.
L1 Substates	Disabled / L1.1 / L1.1 & L1.2	PCI Express L1 Substates settings.
ACS	Enabled / Disabled	Enable or Disable Access Control Services extended capability.
PTM	Enabled / Disabled	Enable or Disable Precision Time Measurement.
FOM Scoreboard Control Policy	Auto / Gen3 / Gen4 / Gen3/Gen4 / Gen5	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
URR	Enabled / Disabled	PCI Express Unsupported Request Reporting enable/disable.
FER	Enabled / Disabled	PCI Express Device Fatal Error Reporting enable/disable.
NFER	Enabled / Disabled	PCI Express Device Non-Fatal Error Reporting enable/disable.
CER	Enabled / Disabled	PCI Express Device Correctable Error Reporting enable/disable.
SEFE	Enabled / Disabled	Root PCI Express System Error on Fatal Error enable/disable.
SENFE	Enabled / Disabled	Root PCI Express System Error on Non-Fatal Error enable/disable.
SECE	Enabled / Disabled	Root PCI Express System Error on Correctable Error enable/disable.
PME SCI	Enabled / Disabled	PCI Express PME SCI enable/disable.
Hot Plug	Enabled / Disabled	PCI Express Hot Plug enable/disable.
PCIe Speed	Auto / Gen1 / Gen2 / Gen3 / Gen4	Configure PCIe Speed.
Detect Timeout	[X]	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
Assertion on Link Down GPIOs	Enabled / Disabled	GPIO Assertion on Link Down
LTR	Enabled / Disabled	PCH PCIE Latency Reporting enable/disable.
Snoop Latency Override	Auto / Manual / Disabled	Snoop Latency Override for PCH PCIE. Disabled: Disable override Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Auto / Manual / Disabled	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
LTR Override Spec Complaint	Spec Complaint - 400ns / Desired Value - from BIOS option	By default is Desired Value. When Desired Value is selected, LTR value will be programmed with recommended value. When Spec Complaint is selected, it will program 400ns LTR value and may block platform PG.
P2P Support	Enabled / Disabled	Program P2P Support Register according to setup option
PCIe EQ settings	See submenu	PCIe EQ settings

Setup Utility ⇨ Advanced ⇨ PCIE Configuration ⇨ PCIE Express Root Port X ⇨ PCIe EQ settings

Menu Item	Options	Description
PCIe EQ override	[X]	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process
PCET Timer	2 ms – 23 ms	Preset/Coefficient Evaluation Timeout – PCET Timer
PCIe EQ mode	Use presets during EQ / Use coefficients during EQ	Choose EQ mode. Preset mode – root port will use presets during EQ process, Coefficient mode – root port will use coefficients during EQ process
EQ PH1 downstream port transmitter preset	[X]	Choose the value of the preset that will be used during phase 1 of the equalization
EQ PH1 upstream port transmitter preset	[X]	Choose the value of the preset that will be used during phase 1 of the equalization
Number of Preset/Coeff List	[X]	Select how many presets or coefficients. Please not that you have to set all of the list entries to valid values. The interpretation of this field depends on PCIe EQ mode
Preset 0 - 10	[X]	Choose the target preset value
PCIe EQ override	[X]	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process
PCET Timer	2 ms – 23 ms	Preset/Coefficient Evaluation Timeout – PCET Timer
PCIe EQ mode	Use presets during EQ / Use coefficients during EQ	Choose EQ mode. Preset mode – root port will use presets during EQ process, Coefficient mode – root port will use coefficients during EQ process
EQ PH1 downstream port transmitter preset	[X]	Choose the value of the preset that will be used during phase 1 of the equalization
EQ PH1 upstream port transmitter preset	[X]	Choose the value of the preset that will be used during phase 1 of the equalization
Number of Preset/Coeff List	[X]	Select how many presets or coefficients. Please not that you have to set all of the list entries to valid values. The interpretation of this field depends on PCIe EQ mode
Preset 0 - 10	[X]	Choose the target preset value
PCIe EQ override	[X]	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process
PCIe EQ override	[X]	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process
PCET Timer	2 ms – 23 ms	Preset/Coefficient Evaluation Timeout – PCET Timer
PCIe EQ mode	Use presets during EQ / Use coefficients during EQ	Choose EQ mode. Preset mode – root port will use presets during EQ process, Coefficient mode – root port will use coefficients during EQ process
EQ PH1 downstream port transmitter preset	[X]	Choose the value of the preset that will be used during phase 1 of the equalization
EQ PH1 upstream port transmitter preset	[X]	Choose the value of the preset that will be used during phase 1 of the equalization
Number of Preset/Coeff List	[X]	Select how many presets or coefficients. Please not that you have to set all of the list entries to valid values. The interpretation of this field depends on PCIe EQ mode
Preset 0 - 10	[X]	Choose the target preset value

6.6.2.10 PCH-IO Configuration

Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration

Menu Item	Options	Description
USB Configuration	See submenu	USB Configuration settings.
Security Configuration	See submenu	Security Configuration settings
HD Audio Configuration	See submenu	HD Audio Subsystem Configuration Settings.
Seriallo Configuration	See submenu	Seriallo Configuration Settings
EFI Network	Onboard NIC / WiFi / Onboard NIC & WiFi / Disabled	Enable/Disable EFI Network support for onboard LAN or WiFi module.
Wake on WLAN and BT Enable	Enabled / Disabled	Enable / Disable PCI Express Wireless LAN and Bluetooth to wake the system.
State After G3	S0 State / S5 State	Specify what state to go to when power is re-applied after a power failure (G3 state).
LPM S0i2.0	Enabled / Disabled	Enable/Disable S0ix sub-state. This setting is for test purpose. S0ix sub-states should be enabled for production.
LPM S0i2.1	Enabled / Disabled	Enable/Disable S0ix sub-state. This setting is for test purpose. S0ix sub-states should be enabled for production.
LPM S0i2.2	Enabled / Disabled	Enable/Disable S0ix sub-state. This setting is for test purpose. S0ix sub-states should be enabled for production.
Enable TCO Timer	Enabled / Disabled	Enable/Disable TCO timer. When disabled, it disables PCH ACPI timer, stops TCO timer, and ACPI WDAT table will not be published
IOAPIC 24-119 Entries	Enabled / Disabled	Enable/Disable IOPIC 24-119 Entries. IRQ24-119 may be used by PCH devices. Disabling those interrupts may cause certain devices failure.
Enable 8254 Clock Gate	Enabled / Disabled	Enable/Disable 8254 glock gate in early phase. Set 8254CGE is necessary for SLP_S0 support. Platform is able to disable this policy and set 8254CGE in late phase.
Lock PCH Sideband Access	Enabled / Disabled	Lock PCH Sideband access, include SideBand interface lock and SideBand PortID mask for certain end point (e.g. PSFx). The option is invalid if POSTBOOT SAL is set.
Flash Protection Range Registers (FPRR)	Enabled / Disabled	Enable Flash Protection Range Registers.
SPD Write Disable	True / False	Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.
LGMR	Enabled / Disabled	64KB memory block for LGMR (LPC Memory Range Decode)
OS IDLE Mode	Enabled / Disabled	Enable/Disable OS idle Mode Feature.
SOix Auto Demotion	Enabled / Disabled	Enable/Disable Host Low Power Mode SOix Auto-Demotion

Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ USB Configuration

Menu Item	Options	Description
xDCI Support	Enabled / Disabled	Enable/Disable xDCI (USB OTG Device)
USB PDO Programming	Enabled / Disabled	Select 'Enabled' if Port Disable override functionality is used.
USB Overcurrent	Enabled / Disabled	Select 'Disabled' for pin-based debug. If pin based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.
USB Overcurrent Lock	Enabled / Disabled	Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data.
USB Audio Offload	Enabled / Disabled	Enable/Disable USB Audio Offload functionality.
Enable HSII on xHCI	Enabled / Disabled	Enable/Disable HSII feature. It may lead to increased power

Menu Item	Options	Description
		consumption.
USB3.1 Portx Speed Selection	[X]	USB3.1 Speed selection; Gen1 or Gen2
USB Port Disable Override	Enabled / Disabled	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.
USB SW Device Mode Port #x	Enabled / Disabled	Enable Connector Event for device subscription.

Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ Security Configuration

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

Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ HD Audio Configuration

Menu Item	Options	Description
HD Audio	Enabled / Disabled	Control detection of the HD-Audio device. Disabled: HAD will be unconditionally disabled. Enabled: HAD will be unconditionally enabled.
Audio DSP	Enabled / Disabled	Enable or disable Audio DSP.
Audio DSP Compliance Mode	Non-UAA (IntelSST) / UAA (HDA Inbox/IntelSST)	Specifies DSP enabled system compliance: 1. Non-UAA (IntelSST driver support only – CC_040100) 2. UAA (HD Audio Inbox or IntelSST driver support – CC_040380) Note: NHLT (DMIC/BT/I2S configuration) is published for non-UAA omly.
HDA Link	Enabled / Disabled	Muxed interfaces: 1) HDA/SSP0 2) HDA[SDI1]/SSP1 3) DMIC0/SNDW3 4) DMIC1/SNDW3 CNL only: 5) HDA/SNDW0 6) SSP1(SNDW1
SDIx	Enabled / Disabled	Muxed interfaces: 1) HAD/SSP0 2) HAD[SDI1]/SSP1 3) DMIC0/SNDW3 4) DMIC1/SNDW3 CNL only: 5) HAD/SNDW0 6) SSP1(SNDW1
DMIC #x	Enabled / Disabled	Muxed interfaces: 1) HAD/SSP0 2) HAD[SDI1]/SSP1 3) DMIC0/SNDW3 4) DMIC1/SNDW3 CNL only: 5) HAD/SNDW0 6) SSP1(SNDW1
SSP #x	Enabled / Disabled	Muxed interfaces: 1) HAD/SSP0

Menu Item	Options	Description
		2) HAD[SDI1]/SSP1 3) DMIC0/SNDW3 4) DMIC1/SNDW3 CNL only: 5) HAD/SNDW0 6) SSP1(SNDW1
SNDW #x	Enabled / Disabled	Muxed interfaces: 1) HAD/SSP0 2) HAD[SDI1]/SSP1 3) DMIC0/SNDW3 4) DMIC1/SNDW3 CNL only: 5) HAD/SNDW0 6) SSP1(SNDW1
SNDW #0 Multilane	Enabled / Disabled	Muxed interfaces: 1) HAD/SSP0 2) HAD[SDI1]/SSP1 3) DMIC0/SNDW3 4) DMIC1/SNDW3 CNL only: 5) HAD/SNDW0 6) SSP1(SNDW1
HD Audio Advanced Configuration	See submenu	HD Audio Subsystem Advanced Configuration Settings
HD Audio Bus Controller Subsystem Id	Default / 72708086 / 300010EC – 306610EC	Selects HD Audio Bus Controller Subsystem Id
HDA Codec ALC256 Configuration	No Dmic to codec / 4 Dmic to codec / 2 Dmic to codec	Option for configuring DMIC connection to ALC256.
SoundWire codecs topology	Default codecs topology / Configuration 305610EC ALC711-VD1, ALC714-VC1, 2x ALC316 / 4-Star Configuration 10EC3044 / 3-Star Configuration 10EC3046 / 2-Star Configuration 10EC3048 / Portofino codecs card / Cirrus 4-speaker configuration / Cirrus 6-speaker Configuration / Disabled	Option allow to select SoundWire codecs topology. Based on connected codecs topology and selected SSID user should select proper ACPI definitions which be exposed in OS.

Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ HD Audio Configuration ⇨ HD Audio Advanced Configuration

Menu Item	Options	Description
iDisplay Audio Disconnect	Enabled / Disabled	Disconnects SDI2 signal to hide/disable iDisplay Audio Codec.
Codec Sx Wake Capability	Enabled / Disabled	Capability to detect wake initiated by a codec in Sx (eg by modem codec)
PME Enable	Enabled / Disabled	Enables PME wake of HD Audio Controller during POST.
Statically Switchable BCLK Clock Frequency Configuration:		Statically Switchable BCLK Clock Frequency Configuration:
HD Audio Link Frequency	6 MHz / 12 MHz / 24 MHz	Selects HD Audio Link frequency. Applicable only if HDA codec supports selected frequency.

Menu Item	Options	Description
iDisplay Audi Link Frequency	48 MHz / 96 MHz	Selects iDisplay Link frequency
iDisplay Audio Link T-Mode	1T Mode / 2T Mode / 4T Mode / 8T Mode / 16T Mode	Indicates whether SDI is operating in 1T, 2T (CNL) or 2T, 4T, 8T mode (ICL).
Autonomous Clock Stop SNDW #x	Enabled / Disabled	Enable/Disable Autonomous Clock Stop for SoundWire LINKx
Data On Active Interval Select SNDW #x	6 clock periods / 7 clock periods / 8 clock periods / 11 clock periods	Data On Active Interval Select: 1) 6 clock periods 2) 7 clock periods 3) 8 clock periods 4) 11 clock periods 5)
Data On Delay Select SNDW #x	2 clock periods / 3 clock periods	Data On Delay Select: 1) 2 clock periods 2) 3 clock periods 3)

Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ Seriallo Configuration

Menu Item	Options	Description
I2C1 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI SFG Space will still 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, SPI0, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when: 1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
I2C2 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI SFG Space will still 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, SPI0, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when: 1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
I2C3 Controller	Enabled / Disabled	Note: I3C cannot be enabled if I2C#3 is enabled due to an ITSS requirement that there are at most 4 unique IRQs per Device, whereas D21 has 5 functions
I2C4 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller For I2C5 and UART2 to work this device has to be enabled
I2C5 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller For this device to work I2C has to be enabled
SPI0 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI SFG Space will still 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, SPI0, 1

Menu Item	Options	Description
		UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when: 1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
SPI1 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI SFG Space will still 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, SPI0, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when: 1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
SPI2 Controller	Disabled	Enables/Disables Seriallo SPI2 Controller The following device depends from: Thermal Subsystem in PCI mode Otherwise SPI2 will not appear in the OS
UART0 Controller	Enabled / Disabled / Communication port (COM)	Set UART0 mode - DBG used for BIOS log print and/or Kernel OS Debug - COM – 16550 compatible serial port with Power Gating support
UART1 Controller	Enabled / Disabled / Communication port (COM)	Enables/Disables Seriallo Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI SFG Space will still 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, SPI0, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when: 1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
UART2 Controller	Enabled / Disabled / Communication port (COM)	Enables/Disables Seriallo Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI SFG Space will still 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, SPI0, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when: 1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
GPIO IRQ Route	IRQ14 / IRQ15	Route all GPIOs to one of the IRQ.
Serial IO I2CX Settings	See submenu	Configure Seriallo Controller
Serial IO UARTX Settings	See submenu	Configure Seriallo Controller
WITT/MITT I2C Test Device	Enabled / Disabled	Enable/Disable I2C WITT Test Device
WITT/MITT I3C Test Device	Enabled / Disabled	Enable/Disable I3C WITT Test Device
WITT/MITT SPI Test Device	Enabled / Disabled	Enable/Disable SPI WITT Test Device
UART Test Device	Disabled / Enabled – UART0 / Enabled – UART1 / Enabled – UART2	Choose if UART Test Device is used and with which controller
Additional Serial IO devices	[X]	When enabled, ACPI will report additional devices connected to Serial

Menu Item	Options	Description
		IO.
SerialIO timing parameters	[X]	Enables additional timing parameters for all SerialIO controllers. Defaults can be changed in each controller setting. Platform restart required to apply changes

Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ Seriallo Configuration⇨ Serial IO I2CX Settings

Menu Item	Options	Description
Connected device	[X]	Indicates what type of device is connected to this Seriallo controller 1: TouchPad 2: TouchPanel 3: Both TouchPad and TouchPanel

Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ Seriallo Configuration ⇨ Serial IO UARTX Settings

Menu Item	Options	Description
Hardware Flow Control	Enabled / Disabled	When enabled configures additional 2 GPIO pads for use as RTS/CTS signals for UART
DMA Enable	Enabled / Disabled	Enabled: UART OS driver will use DMA when possible. Disabled: OS driver will enforce PI0 mode
Power Gating	Auto / Enabled / Disabled	Disabled: No _PS0 _PS3 support, device is left in D0, after initialization Enabled: _PS0 and _PS3 that supports getting device out of reset Auto: _PS0 and _PS3 detection through ACPI if device was initialized prior to first PG. If it was used (DBG2) PG is disabled

6.6.2.11 PCH-FW Configuration

Setup Utility ⇨ Advanced ⇨ PCH-FW Configuration

Menu Item	Option	Description
ME State	Enabled / Disabled	When Disabled, ME will be put into ME Temporarily Disabled Mode. Note: Once this option is changed and saved, it is grayed out to prevent command been sent again before reset.
ME Unconfig on RTC Clear	Enabled / Disabled	When Disabled ME will not be unconfirmed on RTC Clear
Core Bios Done Message	Enabled / Disabled	Enable/Disable Core Bios Done message sent to ME
CSE Data Resilience Support	Enabled / Disabled	Enable/Disable CSE Data Resilience Support
FD0 Shipment State Override	Enabled / Disabled	Enable/Disable FD0 Shipment Sate Override. BIOS will override soft strap setting when enabled
Firmware Update Configuration	See submenu	Configure Management Engine Technology parameters
Extend CSME Measurement to TPM-PCR	Enabled / Disabled	Enable/Disable Extend CSME Measurement to TPM-PCR[0] and AMT Config to TPM-PCR[1]

Setup Utility ⇨ Advanced ⇨ PCH-FW Configuration ⇨ Firmware Update Configuration

Menu Item	Option	Description
Me FW Image Re-Flash	Enabled / Disabled	Enable/Disable Me FW Image Re-Flash function. This option is only valid for next boot.
FW Update	Enabled / Disabled	Enable/Disable ME FW Update function.

6.6.2.12 Platform Settings

Setup Utility ⇨ Advanced ⇨ Platform Settings

Menu Item	Option	Description
Scan Matrix Keyboard Support	Enabled / Disabled	Enables/Disables Scan Matrix Keyboard Support
HID Event Filter Driver	Enabled / Disabled	Enables/Disables HID Event Filter Driver interface to OS.
System Firmware Update Config	See submenu	Config settings for System Firmware Update (Capsule Update)
TCSS Platform Setting	See submenu	Configure TCSS Platform Setting

Setup Utility ⇨ Advanced ⇨ Platform Settings ⇨ System Firmware Update Config

Menu Item	Option	Description
Restore Setup Default	Enabled / Disabled	Restore Setup default settings after System Firmware Update
Skip Power Check	Enabled / Disabled	Skip AC/DC Check before System Firmware Update

Setup Utility ⇨ Advanced ⇨ Platform Settings ⇨ TCSS Platform Setting

Menu Item	Option	Description
Disable TBT PCIE Tree BME	Enabled / Disabled	Recommend enabling “VT-d”, “DMA Control Guarantee” and “Control Iommu Pre-boot Behavior” options along with this.
USBC connector manager selection	Enable UCMC / Enable UCSI 2.0 / Enable UCSI 1.2 / Disabled	Select UCSI or UCMC device in ACPI support based on configuration
Aux Ori Override	Enabled / Disabled	Aux Ori Override
Type C retime TX Compliance Mode	Enabled / Disabled	Default is disable Compliance Mode. Change to Enabled for Type C retime Tx Compliance Mode testing.
BIOS-TCSS handshake	Enabled / Disabled	Enable/Disable BIOS TCSS handshake messages. Disabled: TCSS handshake disabled Enabled: TCSS handshake with either EC or PMC is enabled based on the board ID
Timeout for EC USB enumeration message	[X]	BIOS-EC handshake message USBC_GetUSBCConnStatus timeout value in milli seconds
USBC and USBA Wake Capability	S3 / S4	USBC and USBA Wake Capability
PD PS_ON mode selection	Enable PD/PD-less PS_ON / Disabled	Select TCSS PD Policy on Low Power Entry
Type C Port 1 Conv to TypeA	Enabled / Disabled	Enable / Disable Type C Port 1 Convert to TypeA
Type C Port 2 Conv to TypeA	Enabled / Disabled	Enable / Disable Type C Port 2 Convert to TypeA
Type C Port 3 Conv to TypeA	Enabled / Disabled	Enable / Disable Type C Port 3 Convert to TypeA

Menu Item	Option	Description
Type C Port 4 Conv to TypeA	Enabled / Disabled	Enable / Disable Type C Port 4 Convert to TypeA
Thunderbolt™ Configuration	See submenu	Thunderbolt™ Related Configuration
USBC DataRole Swap Platform Disable Option	TRUE / FALSE	Enable/Disable setting USBC DataRole Swap Platform Disable Option

Setup Utility ⇨ Advanced ⇨ Platform Settings ⇨ TCSS Platform Setting ⇨ Thunderbolt™ Configuration

Menu Item	Option	Description
PCIE Tunneling over USB4	Enabled / Disabled	Enable or disable PCIE Tunneling over USB4
USB4 CM Mode	Firmware CM / Software CM / OS Dependent / CM Debug	FW CM – The system boots with FW CM in both BIOS and OS phase. SW CM – The system boots with SW CM in BIOS phase on OS preference for backward and forward compatible. OS dependent – The system will boot with SW CM in BIOS phase after saving this setting, then boot to OS based on OS preference the reflect to CM setting to next BIOS boot. CM debug – The system with boot without any CM in BIOS phase, then boot to OS with the CM based on OS preference by every boot.
Integrated Thunderbolt™ Enable	Enabled / Disabled	Enable or Disable Integrated Thunderbolt™
Integrated Thunderbolt™ Configuration	See submenu	Integrated Thunderbolt™ Related Configuration

Setup Utility ⇨ Advanced ⇨ Platform Settings ⇨ TCSS Platform Setting ⇨ Thunderbolt™ Configuration ⇨ Integrated Thunderbolt™ Configuration

Menu Item	Option	Description
Os Native Resource Balance	Enabled / Disabled	Os Native Resource Balance
Connect Topology Timeout value for ITBT	[X]	Connect Topology Timeout value for Integrated Thunderbolt™ Controller
Force Poweron Timeout value for ITBT	[X]	Force Poweron Timeout value for Integrated Thunderbolt™ Controller
ITBT RTD3	Enabled / Disabled	ITBT RTD3 Enable/Disable. Note: ITBT RTD3 Disabled is not supported when SW CM is applied for OS
ITBT RTD3 EXIT DELAY	[X]	ITBT RTD3 EXIT DELAY (milli seconds)
PCIE RTD3 POLLING LINK ACTIVE TIMEOUT	[X]	ADJUST LINK ACTIVE POLLING TIME DURING D3C EXIT AND DELAY IN PS0 BEFORE RETURN TO OS (milli seconds)
ITBT Root Port 3 Configuration	See submenu	ITBT Root Port 3 Configuration

Setup Utility ⇨ Advanced ⇨ Platform Settings ⇨ TCSS Platform Setting ⇨ Thunderbolt™ Configuration ⇨ Integrated Thunderbolt™ Configuration ⇨ ITBT Root Port 3 Configuration

Menu Item	Option	Description
ITBT Root Port 3	Enabled / Disabled	None
Extra Bus Reserved	[X]	Extra Bus Reserved 42. Extra Bus Reserved is required for each layer = (Extra Bus Reserved on the previous layer – 2 – the number of non-hot-plug ports in the current layer) / the number of hot-plug ports in the current layer Example. 2 non-hot-plug ports and 3 hot-plug ports per connected device have Recommend below setting

		1 device = 7 2 device = 25 3 device = 79, disable one iTBT root port 4 device = 224, disable three iTBT root port, and not every hotplug port supports connecting to the next layer of devices etc …
Reserved Memory	[X]	Reserved Memory for this Root Bridge (1-4096) MB
Memory Alignment	[X]	Memory Alignment (0-31 bits)
Reserved PMemory	[X]	Reserved Prefetchable Memory for this Root Bridge (1-32768) MB

6.6.2.13 ACPI D3Cold settings

Setup Utility ⇨ Advanced ⇨ ACPI D3Cold settings

Menu Item	Option	Description
ACPI D3 Cold Support	Enabled / Disabled	Enable/Disable ACPI D3Cold support to be executed on D3 entry and exit. Note: Disable it would affect the Storage D3 setting

6.6.2.14 SIO TQMx86

Setup Utility ⇨ Advanced ⇨ SIO TQMx86

Menu Item	Option	Description
Serial Port x	Enabled / Disabled / Auto	Configure Serial port using options: [Disable] No Configuration [Enable] User Configuration [Auto] EFI/OS chooses configuration
Base I/O Address	2E8 / 2F8 / 3E8 / 3F8	
Interrupt	IRQ3 / IRQ4 /IRQ5 /IRQ6 / IRQ7	
Enable Fan Control	Enabled / Disabled	Enable or Disable Fan Control function
Enable Fan Control	25 Hz / 25 kHz	Enable or Disable Fan Control function
Active Trip Point 0 Fan Speed	40% / 55% / 70% / 85% / 100% / off	Active Trip Point 0 Fan Speed of temperature range 50°C – 59°C. Below 50°C processor temperature the FAN is off. Above 90°C processor temperature the FAN is always on.
Active Trip Point 1 Fan Speed	40% / 55% / 70% / 85% / 100% / off	Active Trip Point 1 Fan Speed of temperature range 60°C – 79°C. Below 50°C processor temperature the FAN is off. Above 90°C processor temperature the FAN is always on.
Active Trip Point 2 Fan Speed	40% / 55% / 70% / 85% / 100% / off	Active Trip Point 2 Fan Speed of temperature range 70°C – 79°C. Below 50°C processor temperature the FAN is off. Above 90°C processor temperature the FAN is always on.
Active Trip Point 3 Fan Speed	40% / 55% / 70% / 85% / 100% / off	Active Trip Point 3 Fan Speed of temperature range 80°C – 89°C. Below 50°C processor temperature the FAN is off. Above 90°C processor temperature the FAN is always on.

6.6.2.15 H20Uve Configuration

Setup Utility ⇨ Advanced ⇨ H20Uve Configuration

Menu Item	Options	Description
H20UVE Support	Enabled / Disabled	Enable/Disable interface of settings of SCU for H20UVE tool.

6.6.2.16 Console Redirection

Setup Utility ⇨ Advanced ⇨ Console Redirection

Menu Item	Options	Description
Console Serial Redirect	Enabled / Disabled	Enable or disable the Console Redirection. This options unhide CR parameters when enabled.

If enabled:

Menu Item	Options	Description
Console Serial Redirect	Enabled	Enable or disable the serial console redirection function.
Terminal Type	PC_ANSI / VT_100 / VT_100+ / VT_UTF8 / LO_TERM / TTY_TERM / LINUX_TERM / XTERM_R6 / VT_400 / SC0_TERM	Select the target terminal emulation type for console redirection.
Baud Rate	115200 / 57600 / 38400 / 19200 / 9600 / 4800 / 2400 / 1200	Select the baud rate for console redirection.
Data Bits	7 Bits / 8 Bits	Select the data transmission size for console redirection
Parity	None / Even / Odd / Mark / Space	Select an option for sending parity bits with regular data bits to detect data transmission errors.
Stop Bits	1 Bit / 2 Bits	Select a stop bit to indicate the end of a serial data packet.
Flow Control	None / RTS/CTS / XON/XOFF	Select the flow control for console redirection.
Text Mode Resolution	AUTO / Force 80×25 / Force 80×24 (DEL FIRST ROW) / Force 80×24 (DEL LAST ROW) / Limit 128x40	Console Redirection Text Mode Resolution. Changing this setting will affect the VGA resolution. Auto: Follow VGA text mode Force 80×25: Don't care VGA, force text mode be 80×25 (VGA 640x480). Force 80×24 (DEL FIRST ROW): Don't care VGA, force text mode be 80×24, Del first row Force 80×24 (DEL LAST ROW): Don't care VGA, force text mode be 80×24, Del last row Limit 128x40: Limit the VGA , max text mode on 128x40 (VGA 1024x768).
Auto adjust Terminal resolution	Enabled / Disabled	Through send extra ESC sequences code to adjust terminal resolution to fit host screen. Supporting terminals: 1. Putty: Please uncheck the "Disable remote –controlled terminal resizing" in Terminal->Features setting. 2. Tera Term: Please check the "Term Size = win size" in Setup->Terminal.

6.6.3 Security

Setup Utility ⇨ Security

Menu Item	Options	Description
TrEE Protocol Version	1.0 / 1.1	TrEE Protocol Version: 1.0 or 1.1.
TPM Availability	Available / Hidden	When Hidden, do not exposes TPM to 0S Warning: If Supervisor/User password is verified with TPM, change

Menu Item	Options	Description
		this option will disable password automatically
TPM Operation	No Operation / Enable / SetPCRBanks(Algorithm) / LogAllDigests / SetPPRequiredForClear_True / SetPPRequiredForClear_False / SetPPRequiredForTurnOn_False / SetPPRequiredForTurnOn_True / SetPPRequiredForTurnOff_False / SetPPRequiredForTurnOff_True / SetPPRequiredForChangePCRs_False / SetPPRequiredForChangePCRs_True / SetPPRequiredForChangeEPS_False / SetPPRequiredForChangeEPS_True / ChangeEPS	Select one of the supported operation to change TPM2 state.
Clear TPM	[ ] / [X]	Clear TPM. Removes all TPM context associated with a specific Owner.
Set Supervisor Password	123456	Install or change the password and the length of password must be between 0 and 20 characters.
Set All Hdd Password	123456	Set all HDD password and suggest the length of password greater than one character. This item can be displayed when any security mode of HDD is not Lock. This item can be used for ATA Password Security; TCG Opal Security is not supported be design.
Set Alll Master Hdd Password	123456	Set all master HDD password and suggest the length of password greater than one character. This item can be used when all of HDDs are set HDD password. This item can be used for ATA Password Security; TCG Opal Security is not supported be design.
Storage Password Setup Page	See submenu	Storage Password Setup Page

6.6.4 Power

Setup Utility ⇨ Power

Menu Item	Options	Description
Wake on PME	Enabled / Disabled	Determines the action taken when the system power is off and a PCI Power Management Enable (PME) wake up event occurs.
Wake on Modem Ring	Enabled / Disabled	Determines the action taken when the system power is off and a modem connected to the serial port is ringing.
Auto Wake on S5	Disabled / By Every Day / By Day of Month	Auto wake on S5, By Day of Month or Fixed time of every day.
S5 Long Run Test	Enabled / Disabled	Enable: force to enable RTC S5 wake up, even if OS disables it. Support ipwrtest to do RTC S5 wakeup.

6.6.5 Boot

Setup Utility ⇨ Boot

Menu Item	Options	Description
Quick Boot	Enabled / Disabled	Allow InsydeH2O to skip certain tests while booting. This will decrease the time needed to boot the system.
Quite Boot	Enabled / Disabled	Enable or disable booting in Text mode. No textual outputs are given while booting if this option is disabled.
Network Stack	Enabled / Disabled	Enable or disable Network stack Support: Windows 8 BitLocker Unlock UEFI IPv4/IPv6 PXE Legacy PXE OPROM Note: This option will grey-out the PXE Boot capability option.
Power Up In Standby Support	Enabled / Disabled	Disable or enable Power Up In Standby Support. The PUIS feature set allows devices to be powered-up into the Standby power management state to minimize inrush current at power-up and to allow the host to sequence the spin-up of devices.
Storage PCI Option Rom access right Support	Enabled / Disabled	Disable or enable storage PCI option rom access right. This feature will enable or disable storage PCI option rom being load and dispatched.
ESATA drive boot access right Support	Enabled / Disabled	Disable or enable ESATA drive boot access right. This feature will allow or deny boot up an ESATA storage device.
Add Boot Options	First / Last / Auto	The policy of how to insert new boot option into Boot Order. If boot options are not grouped, Auto is the same as First.
ACPI Selection	Acpi1.3.0 / Acpi4.0 / Acpi5.0 / Acpi6.0 / Acpi6.1 / Acpi6.2 / Acpi6.3 / Acpi6.4	Select booting to Acpi1.3.0/Acpi4.0/Acpi5.0/Acpi6.0/Acpi6.1/Acpi6.2/Acpi6.3/Acpi6.4
USB Boot	Enabled / Disabled	Enable or disable booting to USB boot device.
UEFI OS Fast Boot	Enabled / Disabled	If enabled the system firmware does not initialize keyboard and check for firmware menu key.
USB Hot Key Support	Enabled / Disabled	Enable or disable to support USB hot key while booting. This will decrease the time needed to boot the system.
Timeout	[X]	The number of seconds that the firmware will wait before booting the original default boot selection.
Automatic Failover	Enabled / Disabled	Enable: If boot to default device fail, it will directly try to boot next device. Disable: If boot to default device fail, it will pop warning message then go into firmware UI.
Group Boot Options	Grouped / Non-Grouped	Boot options are grouped or not.
Sync Order	Disabled / Sync Boot Order / Sync Boot Device Type Order	Disabled: No effect. Sync Boot Order: Group boot options in Boot Order is adjusted to follow boot device type priority. Sync Boot Device Type Order: Boot device type order is adjusted to follow the order of group boot options in Boot Order.
Adjust Non-BIOS Boot Options	Enabled / Disabled	When enabled, position of Non-BIOS created boot options will be adjusted to follow boot options positon policy each time before enumerate boot devices.
Group Auto Boot Order	Enabled / Disabled	When enabled, keep boot option order of each group in “Auto” position policy.
Device Type in Boot Manger	Enabled / Disabled	Enabled: Show Boot Device Type Label in Boot Manger. Disabled: Hide Boot Device Type Label in Boot Manger.

6.6.6 Exit

Setup Utility ⇨ Exit

Menu Item	Option	Description
Exit Saving Changes		Exit system setup and save your changes.
Save Change Without Exit		Save your changes and without exiting system.
Exit Discarding Changes		Exit system setup and without saving your changes.
Load Optimal Defaults		Load Optimal defaults.
Save Custom Defaults		Save Custom defaults.
Discard Changes		Discard Changes.

6.6.7 BIOS Update

The UEFI BIOS update instruction serves to guarantee a proper way to update the UEFI BIOS on the TQMxCU1-HPCM.
Please read the entire instructions before beginning the BIOS update.
By disregarding the information, you can destroy the UEFI BIOS on the TQMxCU1-HPCM!
This document will guide the user to update the UEFI BIOS on the TQMxCU1-HPCM by using the Insyde Flash Firmware Tools.
The InsydeH2O Tools are only available on request.
Please contact TQ-Support for more information about the BIOS Tools and the latest UEFI BIOS version for the TQMxCU1-HPCM.

Note: Installation procedures and screen shots	
	Installation procedures and screen shots in this section are for your reference and may not be exactly the same as shown on your screen.

Step 1: Preparing USB Stick

A FAT32 formatted USB stick can be used. Copy the following files to the USB stick.

- H2OFFT-Sx64.efi (Flash Firmware Tool from Insyde for update via UEFI Shell)
  - Be sure to have H2OFFT Version 200.02.00.06 or later
- InsydeH2OFF_x86_WINx64 folder (Flash Firmware Tool from Insyde for update via Windows 64-bit system)
- BIOS binary file, e.g. xx.bin

See: https://www.tq-group.com/en/support/downloads/tq-embedded/software-drivers/x86-architecture/

Step 2: Preparing Management Engine (ME) FW for update

Enter the BIOS menu by pressing <ESC> while booting (POST phase) and navigate to the following page:

Setup Utility ⇨ Advanced ⇨ PCH-FW Configuration ⇨ Firmware Update Configuration

Then, set option “ME FW Image Re-Flash” to “enabled”, save and exit by pressing <F10> and <Enter>.

Note: Option availability	
	This option will only be valid for the next boot.

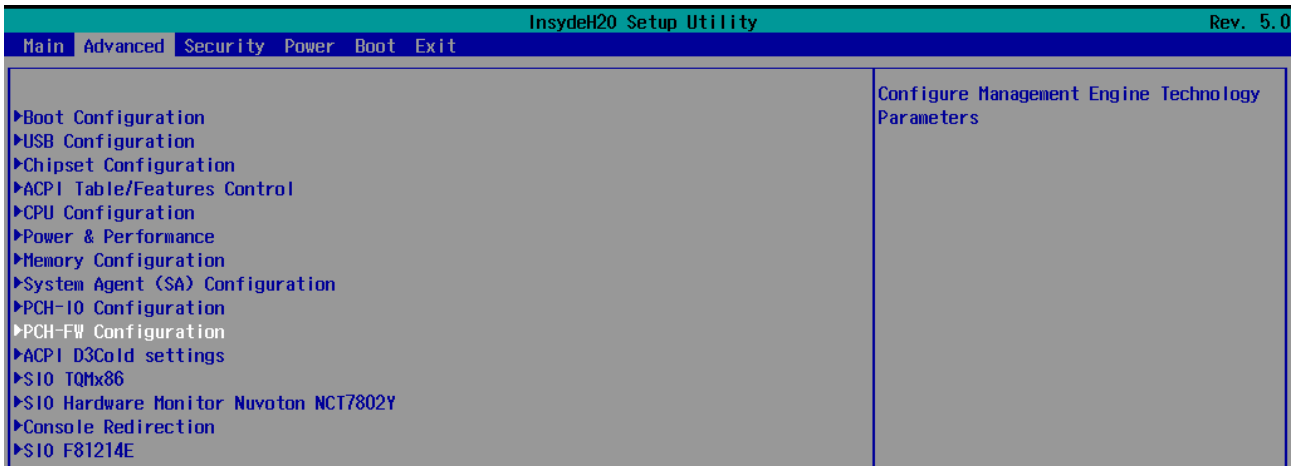

Figure 11: PCH-FW Configuration Menu

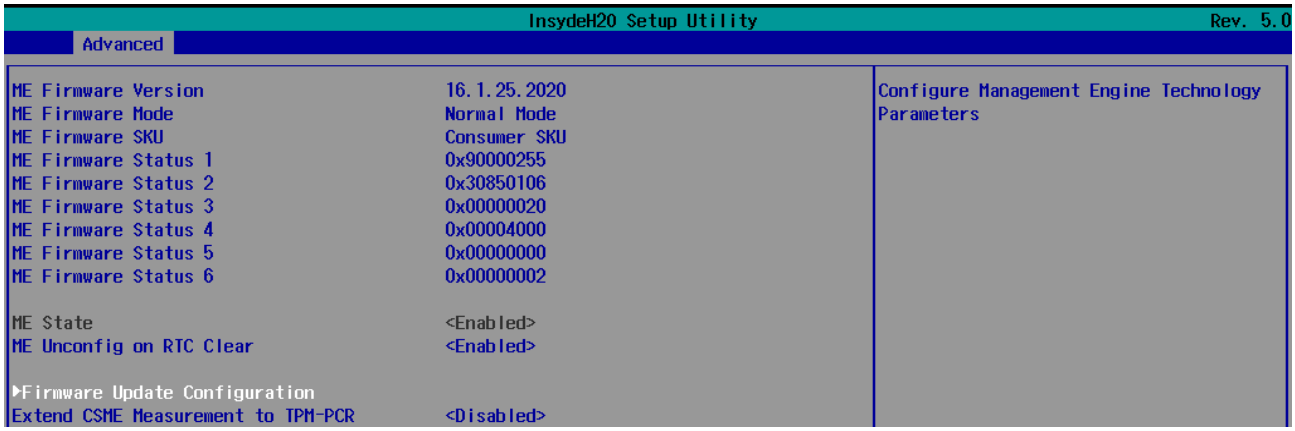

Figure 12: Firmware Update Configuration Menu

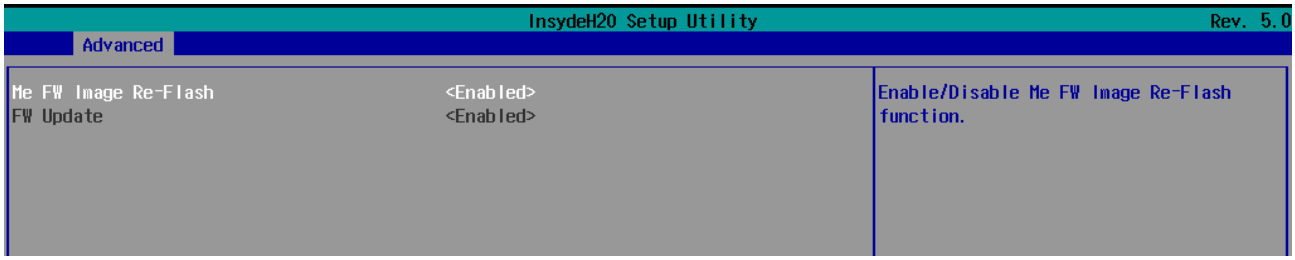

Figure 13: ME FW Image Re-Flash Option

Step 3a: Updating UEFI BIOS via EFI Shell

Plug the USB stick into the board on which you want to update the UEFI BIOS and power up the board. The board will boot and go to the internal EFI shell.
Note: If a boot device is connected, change to “Boot Manager” via Front Page and select “Internal EFI Shell”.

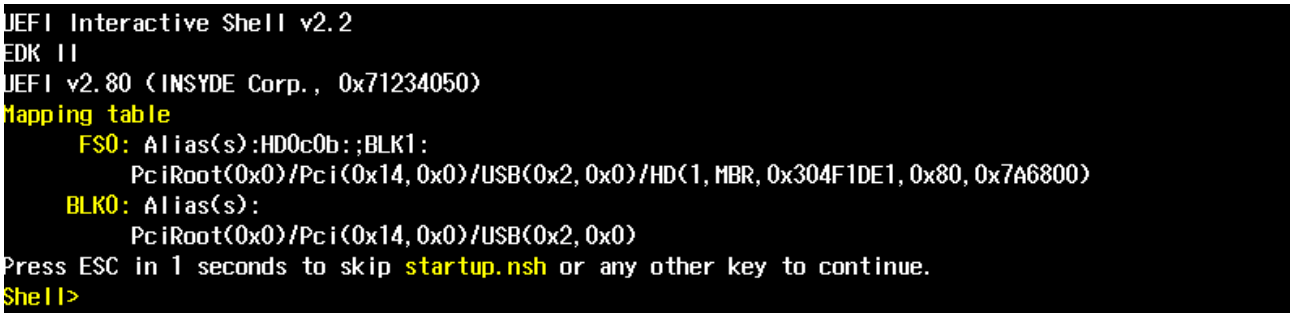

Figure 14: EFI Shell

Please see device mapping table on the screen and select the removable hard disk file system "fsX" (X = 0, 1, 2, …).
Move operating directory to USB drive with e.g. "`fs0:`"
Then, navigate to the BIOS folder (e.g. "`cd TQMxCU1-HPCM`") to execute the Insyde BIOS update tool:

```
H2OFFT-Sx64.efi <BIOS file> -all -ra
```

If the option "`-ra`" is set, the SMBIOS data will not be overwritten and the UUID included in SMBIOS data will be preserved. However, this argument is not mandatory.

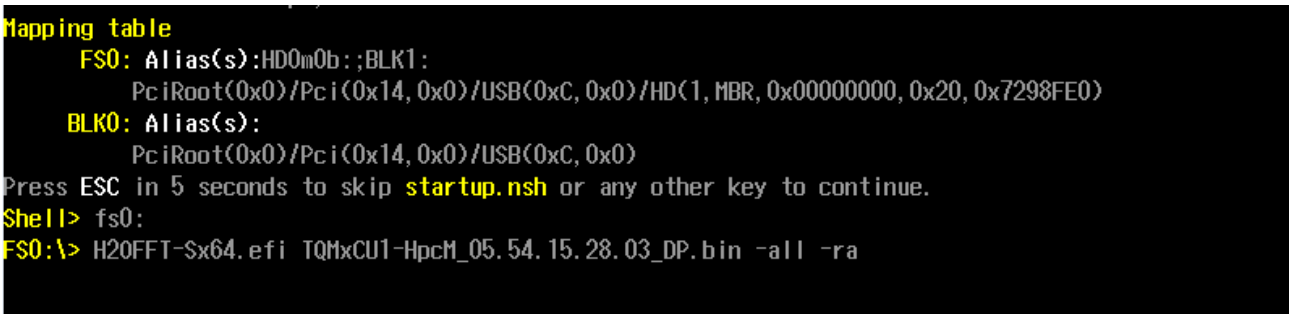

Figure 15: EFI Shell UEFI BIOS Update

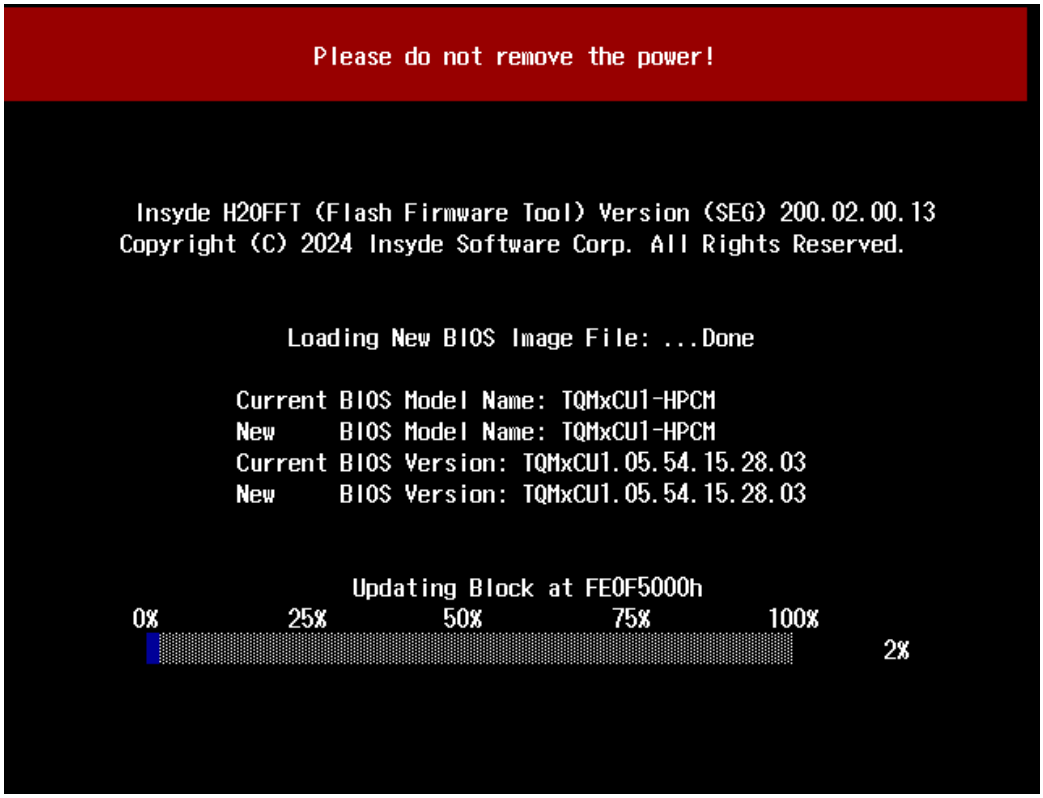

Figure 16: Screen during BIOS Update

Step 3b: Updating UEFI BIOS via Windows Operating System

Boot the Windows operating system (64-bit) and insert the USB stick into the board on which you want to update the UEFI BIOS. Start the Command Prompt (CMD). It is important to note that the Command Prompt must be started in the administrator mode!

Select the BIOS update folder with the Insyde Windows 64-bit update tool and execute the Insyde BIOS update tool.

```
H2OFFT-Wx64.exe <BIOS file>.bin -all -ra
```

For the <BIOS file> argument, please specify the .bin file with the full path (e.g. D:\TQMxXXXX_X.xx.xx.xx.xx.bin).

If the option "`-ra`" is used, the SMBIOS data will not be overwritten and the UUID included in SMBIOS data will be preserved. However, this argument is not mandatory.

Start the BIOS update with the Insyde Windows 64-bit update tool.

Step 4: BIOS update check on the TQMxCU1-HPCM Module

After the UEFI BIOS update, the new UEFI BIOS configures the complete TQMxCU1-HPCM hardware. This results in several reboots and the first boot time takes longer (up to 1 ~ 2 minutes).

The TQMxCU1-HPCM features a dual colour Debug LED providing boot and UEFI BIOS information.

If the green LED blinks, the UEFI BIOS is booting. If the green LED is lit permanently, the UEFI BIOS boot is completed.

Figure 17: TQMxCU1-HPCM Debug LED

After the UEFI BIOS flash is completed, please check whether the UEFI BIOS has been flashed successfully.

The BIOS Main menu provides the board and hardware information and it shows the installed BIOS version.

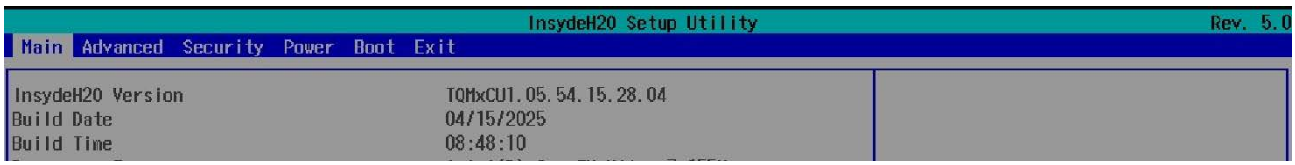

Figure 18: EFI BIOS Main Menu

7. SAFETY REQUIREMENTS AND PROTECTIVE REGULATIONS

7.1 EMC

The TQMxCU1-HPCM was developed according to electromagnetic compatibility requirements (EMC). Depending on the target system, anti-interference measures may still be necessary to guarantee the adherence to the limits for the overall system.

7.2 ESD

In order to avoid interspersion on the signal path from the input to the protection circuit in the system, the protection against electrostatic discharge should be placed directly at the inputs of a system. As these measures always have to be implemented on the carrier board, no special preventive measures were taken on the TQMxCU1-HPCM.

7.3 Shock & Vibration

The TQMxCU1-HPCM is designed to be insensitive to shock, vibration, and impact.

7.4 Operational Safety and Personal Security

Due to the occurring voltages (≤20 V DC), tests with respect to the operational and personal safety have not been carried out.

7.5 Cyber Security

The user must always perform a Threat Analysis and Risk Assessment (TARA) for their individual end application, since the TQMxCU1-HPCM is only a sub-component of an overall system.

7.6 Reliability and Service Life

The MTBF according to MIL-HDBK-217 FN2 is approximately 788,701 hours, Ground Benign, @ +40 °C.

7.7 RoHS

The TQMxCU1-HPCM is manufactured RoHS compliant.

- All components and assemblies are RoHS compliant
- The soldering processes are RoHS compliant

7.8 WEEE®

The company placing the product on the market is responsible for the observance of the WEEE® regulation.
To be able to reuse the product, it is produced in such a way (a modular construction) that it can be easily repaired and disassembled.

7.9 REACH®

The EU-chemical regulation 1907/2006 (REACH® regulation) stands for registration, evaluation, certification and restriction of substances SVHC (Substances of very high concern, e.g., carcinogen, mutagen and/or persistent, bio accumulative and toxic). Within the scope of this juridical liability, TQ-Systems GmbH meets the information duty within the supply chain with regard to the SVHC substances, insofar as suppliers inform TQ-Systems GmbH accordingly.

7.10 Statement on California Proposition 65

California Proposition 65, formerly known as the Safe Drinking Water and Toxic Enforcement Act of 1986, was enacted as a ballot initiative in November 1986. The proposition helps to protect the state's drinking water sources from contamination by approximately 1,000 chemicals known to cause cancer, birth defects, or other reproductive harm ("Proposition 65 Substances") and requires businesses to inform Californians about exposure to Proposition 65 Substances.

The TQ device or product is not designed, manufactured, or distributed as consumer product or for any contact with end-consumers. Consumer products are defined as products intended for a consumer's personal use, consumption, or enjoyment. Therefore, our products or devices are not subject to this regulation and no warning label is required on the assembly.

Individual components of the assembly may contain substances that may require a warning under California Proposition 65. However, it should be noted that the Intended Use of our products will not result in the release of these substances or direct human contact with these substances. Therefore, you must take care through your product design that consumers cannot touch the product at all and specify that issue in your own product related documentation.

TQ-Systems GmbH reserves the right to update and modify this notice, as it deems necessary or appropriate.

7.11 EuP

The Eco Design Directive, also Energy using Products (EuP), is applicable to products for the end user with an annual quantity >200,000.
The TQMxCU1-HPCM must therefore always be seen in conjunction with the complete device. The available standby and sleep modes of the components on the TQMxCU1-HPCM enable compliance with EuP requirements for the TQMxCU1-HPCM.

7.12 Battery

No batteries are assembled on the TQMxCU1-HPCM.

7.13 Packaging

By environmentally friendly processes, production equipment and products, we contribute to the protection of our environment.
To be able to reuse the TQMxCU1-HPCM, it is produced in such a way (a modular construction) that it can be easily repaired and disassembled.
The energy consumption of this subassembly is minimised by suitable measures.
The TQMxCU1-HPCM is delivered in reusable packaging.

7.14 Export Control and Sanctions Compliance

The customer is responsible for ensuring that the product purchased from TQ is not subject to any national or international export/import restrictions. If any part of the purchased product or the product itself is subject to said restrictions, the customer must procure the required export/import licenses at its own expense. In the case of breaches of export or import limitations, the customer indemnifies TQ against all liability and accountability in the external relationship, irrespective of the legal grounds. If there is a transgression or violation, the customer will also be held accountable for any losses, damages or fines sustained by TQ. TQ is not liable for any delivery delays due to national or international export restrictions or for the inability to make a delivery as a result of those restrictions. Any compensation or damages will not be provided by TQ in such instances.
The classification according to the European Foreign Trade Regulations (export list number of Reg. No. 2021/821 for dual-use-goods) as well as the classification according to the U.S. Export Administration Regulations in case of US products (ECCN according to the U.S. Commerce Control List) are stated on TQ´s invoices or can be requested at any time. Also listed is the Commodity code (HS) in accordance with the current commodity classification for foreign trade statistics as well as the country of origin of the goods requested/ordered.

7.15 Warranty

TQ-Systems GmbH warrants that the product, when used in accordance with the contract, fulfils the respective contractually agreed specifications and functionalities and corresponds to the recognized state of the art.
The warranty is limited to material, manufacturing and processing defects. The manufacturer's liability is void in the following cases:

- Original parts have been replaced by non-original parts
- Improper installation, commissioning or repairs
- Improper installation, commissioning or repair due to lack of special equipment
- Incorrect operation
- Improper handling
- Use of force
- Normal wear and tear

7.16 Other Entries

By environmentally friendly processes, production equipment and products, we contribute to the protection of our environment.
The energy consumption of this subassembly is minimised by suitable measures.
Printed PC-boards are delivered in reusable packaging.
Modules and devices are delivered in an outer packaging of paper, cardboard or other recyclable material.
Since there is currently no technical equivalent alternative for printed circuit boards with bromine-containing flame protection (FR-4 material), such printed circuit boards are still used.
No use of PCB containing capacitors and transformers (polychlorinated biphenyls).
These points are an essential part of the following laws:

- The law to encourage the circular flow economy and assurance of the environmentally acceptable removal of waste as at 27.9.94
  (source of information: BGBl I 1994, 2705)
- Regulation with respect to the utilization and proof of removal as at 1.9.96
  (source of information: BGBl I 1996, 1382, (1997, 2860))
- Regulation with respect to the avoidance and utilization of packaging waste as at 21.8.98
  (source of information: BGBl I 1998, 2379)
- Regulation with respect to the European Waste Directory as at 1.12.01
  (source of information: BGBl I 2001, 3379)

This information is to be seen as notes. Tests or certifications were not carried out in this respect.

8. APPENDIX

8.1 Acronyms and Definitions

The following acronyms and abbreviations are used in this document.

Table 19: Acronyms

Acronym	Meaning
AHCI	Advanced Host Controller Interface
BIOS	Basic Input/Output System
CAN	Controller Area Network
CMOS	Complementary Metal Oxide Semiconductor
CODEC	Code/Decode
COM	Computer-On-Module
CPU	Central Processing Unit
CSM	Compatibility Support Module
cTDP	Configurable Thermal Design Power
DC	Direct Current
DDC	Display Data Channel
DDI	Digital Display Interface
DDR	Double Data Rate
DMA	Direct Memory Access
DP	DisplayPort
DVI	Digital Visual Interface
EAPI	Embedded Application Programming Interface
ECC	Error-Correcting Code
EDID	Extended Display Identification Data
eDP	embedded DisplayPort
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFI	Extensible Firmware Interface
EMC	Electromagnetic Compatibility
ESD	Electrostatic Discharge
FAE	Field Application Engineer
FIFO	First In First Out
flexiCFG	Flexible Configuration
FPGA	Field Programmable Gate-Array
FR-4	Flame Retardant 4
FW	Firmware
GPIO	General-purpose Input/Output
HDA	High Definition Audio
HDMI	High Definition Multimedia Interface
HEVC	High Efficiency Video Coding
HSP	Heat Spreader
HT	Hyper-Threading
I	Input
I PD	Input with internal Pull-Down resistor
I PU	Input with internal Pull-Up resistor
I/O	Input/Output
I^2C	Inter-Integrated Circuit
IEC	International Electrotechnical Commission
IoT	Internet of Things
IP00	Ingress Protection 00
IRQ	Interrupt Request
JEIDA	Japanese Electronics Industry Development Association
JPEG	Joint Photographic Experts Group
JTAG®	Joint Test Action Group
LED	Light Emitting Diode
LPDDR5	Low Power Double Data Rate 5
ME	Management Engine
MMC	Multimedia Card
MPEG	Moving Picture Experts Group
MST	Multi-Stream Transport
MT/s	Mega Transfers per second
MTBF	Mean operating Time Between Failures

8.1 Acronyms and Definitions (continued)

Table 19: Acronyms (continued)

Acronym	Meaning
N/A	Not Available
NC	Not Connected
O	Output
OD	Open Drain
OpROM	Option ROM
OS	Operating System
PC	Personal Computer
PCB	Printed Circuit Board
PCH	Platform Controller Hub
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
PD	Pull-Down
PEG	PCI Express for Graphics
PICMG®	PCI Industrial Computer Manufacturers Group
POST	Power-On Self-Test
PU	Pull-Up
PWM	Pulse-Width Modulation
RAID	Redundant Array of Independent/Inexpensive Disks/Drives
RAM	Random Access Memory
RMA	Return Merchandise Authorization
RoHS	Restriction of (the use of certain) Hazardous Substances
RSVD	Reserved
RTC	Real-Time Clock
SATA	Serial ATA
SCU	System Control Unit
SD	Secure Digital
SD/MMC	Secure Digital Multimedia Card
SDIO	Secure Digital Input/Output
SIMD	Single Instruction, Multiple Data
SMART	Self-Monitoring, Analysis and Reporting Technology
SMBus	System Management Bus
SO-DIMM	Small Outline Dual In-Line Memory Module
SPD	Serial Presence Detect
SPI	Serial Peripheral Interface
SPKR	Speaker
SSD	Solid-State Drive
STEP	Standard for Exchange of Products
TDM	Time-Division Multiplexing
TDP	Thermal Design Power
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver/Transmitter
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VC-1	Video Coding (format) 1
VESA	Video Electronics Standards Association
VGA	Video Graphics Array
VP8	Video Progressive (compression format) 8
WDT	Watchdog Timer
WEEE®	Waste Electrical and Electronic Equipment
WES	Windows® Embedded Standard

8.2 References

Table 20: Further Applicable Documents and Links

No.	Name	Rev.	Company
(1)	Intel® Core™ Ultra processor Product Brief	–	Intel
(2)	PICMG® COM-HPC® Module Base Specification	Rev. 1.2	PICMG
(3)	PICMG® COM-HPC® Carrier Design Guide	Rev. 2.2	PICMG PDF
(4)	PICMG® COM-HPC® Embedded Application Programming Interface	Rev. 1.0	PICMG PDF

TQ-Systems GmbH
Mühlstraße 2 l Gut Delling l 82229 Seefeld
info@tq-group.com l www.tq-group.com

Technology in Quality