TQMxE41S
User's Manual

TQMxE41S UM 0100a
08.05.2024

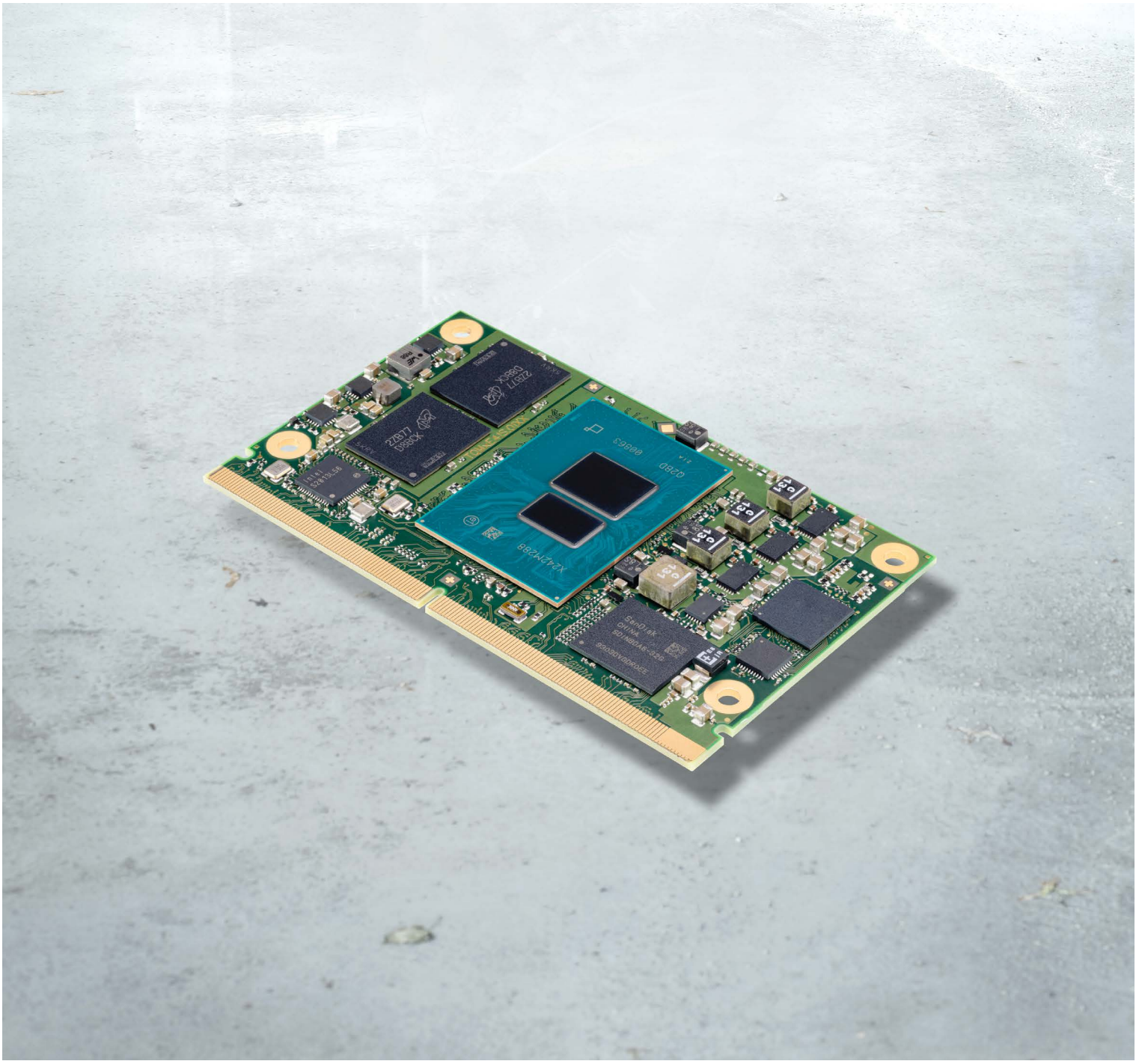

TABLE OF CONTENTS

TABLE DIRECTORY

FIGURE DIRECTORY

REVISION HISTORY

Rev.	Date	Name	Pos.	Modification
0100	11.12.2023	PD		Initial release
0100a	08.05.2024	Kreuzer	Chapter 2	Typo and formatting

1. ABOUT THIS MANUAL

1.1 Copyright and Licence 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 the 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 must 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 Imprint

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

Tel: +49 8153 9308–0
Fax: +49 8153 9308–4223
Email: info@tq-group.com
Web: www.tq-group.com/

1.5 Service and Support

Please visit our website www.tq-group.com for latest product documentation, drivers, utilities and technical support.

Through our website www.tq-group.com you could also get registered, to have access to restricted information and automatic update services.

For direct technical support you could contact our FAE team by email: support@tq-group.com

Our FAE team can support you also with additional information like 3D-STEP files and confidential information which is not provided on our public website.

For service / RMA, please contact our service team by email (service@tq-group.com) or your dedicated sales team at TQ.

1.6 Tips on Safety

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

1.7 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 also 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.

1.8 Handling and ESD Tips

General handling of your TQ-products

	The TQ-product may only be used and serviced by certified personnel who have taken note of the information, the safety regulations in this document and all related rules and regulations. A general rule is: do not touch the TQ-product during operation. This is especially important when switching on, changing jumper settings or connecting other devices without ensuring beforehand that the power supply of the system has been switched off. Violation of this guideline may result in damage / destruction of the TQMxE41S and be dangerous to your health. Improper handling of your TQ-product would render the guarantee invalid.

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.

1.9 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#

1.10 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, for example CompactFlash cards, are to be taken note of. They contain, if applicable, additional information that must 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 followed.
- **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 SMARC Design Guide (2) maintained by the SGET (Standardization Group for Embedded Technologies). This Carrier Design Guide includes a very good guideline to design SMARC carrier board.

It includes detailed information with schematics and detailed layout guidelines.

Please refer to the official SGET documentation for additional information (1).

2. INTRODUCTION

The TQ module TQMxE41S is based on Intel Atom® processor x7000E series, Intel® Core™ i3-N305 and Intel® Processor N-series (code name: Alder Lake-N) and corresponds to the internationally established SGET standard SMARC (V2.1.1). Six USB ports – including two USB 3.0 – and up to four PCIe lanes natively supported by the CPUs enable high bandwidth communication with peripherals and additional interfaces on the carrier board. With the latest Intel® graphics processor integrated, the TQMxE41S delivers 4K high resolution graphics output, immersive 3D processing and also greatly increased video encode and playback performance.

Time coordinated computing capabilities enable time synchronized processes within IoT networks and industrial control applications. On-board eMMC and the option for LVDS or native eDP enable flexibility and reduce overall BOM cost.

The integrated TQMx86 board controller enables high flexibility through "flexiCFG" and supports thermal management, watchdog, 16550 compatible UARTs, I²C controllers, and GPIO handling. Combined with options like conformal coating and optimized cooling solutions the TQMxE41S fits for mobile, low power, low profile and battery driven applications.

2.1 Functional Overview

The following key functions are implemented on the TQMxE41S:

CPU:

- Intel® x7000 Series and Core i3 N-Series: „Alder Lake N" with different SKUs
- optimized for Embedded, Edge Computing or PC Client applications

Memory:

- LPDDR5: 4 Gbyte, 8 Gbyte, 16 Gbyte with up to 4800 MT/s and optional In Band ECC (IBECC)
- eMMC 5.1 on-board flash with up to 256 GB
- EEPROM: 32 kbit

Graphics:

- 2 × Digital Display Interface (DDI) (2x DP or 1x DP and 1x HDMI)
- 1 × Embedded Display Port Interface or LVDS interface (eDP or LVDS)

Peripheral interfaces:

- 2 × 2.5 Gigabit Ethernet (Intel® i226)
- 1 × SATA 3.0 (up to 6 Gb/s)
- 4 × PCIe Gen3 (up to 8 GT/s)
- 2 × USB 3.2 (with up to 10Gb/s and USB 2.0 backward compatibility)
- 6 × USB 2.0 (incl. USB 3.2 ports)
- 1 × Intel® HD audio (HDA) and I²S or 2x I²S
- 1 × I²C (General Purpose)
- 1 × SMBus
- 1 × SPI (for external uEFI BIOS flash)
- 1 x eSPI interface
- 4 × Serial port (Rx/Tx, legacy compatible)
- 14 GPIO signals (multiplexed with fan / camera control and HD audio Reset)

Security components:

- TPM (SLX9670 TPM 2.0)

Others:

- TQMx86 board controller with Watchdog and TQ-flexiCFG

Power supply:

- Voltage: 4.75 V to 5.25 V
  3 V Battery for RTC

Environment:

- Standard Temperature: 0 °C to +60 °C

Form factor / dimensions:

- SMARC short form factor; 82 mm × 50 mm

2.2 SMARC Specification Compliance

The TQMxE41S is compliant to the SMARC Hardware Specification (Version 2.1.1)

2.3 TQMxE41S Variants

The TQMxE41S is available in several standard configurations:

Please visit www.tq-group.com/TQMxE41S for a complete list of standard variants.
Other configurations are available on request.

Standard configuration features are:

- eDP or LVDS
- 2x DP++ or 1x DP++ and HDMI
- CPU version
- Memory configuration (RAM / eMMC)
- TPM

Optional hardware and software configuration features:

- Conformal coating can be offered as custom specific add-on
- Custom specific GPIO configuration through TQ-flexiCFG
- Custom specific BIOS configuration

2.4 Accessories

TQMxE41S-HSP: Heat spreader for TQMxE41S according to the SMARC specification
Evaluation platform MB-SMARC-3:

- Mainboard for SMARC modules
- 170 mm × 170 mm
- Interfaces:
  - DP++, HDMI 2.0, eDP/LVDS,
  - 2 × GbE
  - 1 × USB Type C, 1 x USB 3.0, 1 x USB 2.0
  - HDA and I^2S Audio
  - Micro SD card (not applicable with TQMxE41S)
  - 3 x M.2 socket (Key B, E, M), PCIe socket
  - up to 6 serial interfaces
  - 2 × CAN (not applicable with TQMxE41S)

3. FUNCTION

3.1 TQMxE41S Block Diagram

The following illustration shows the block diagram of the TQMxE41S:

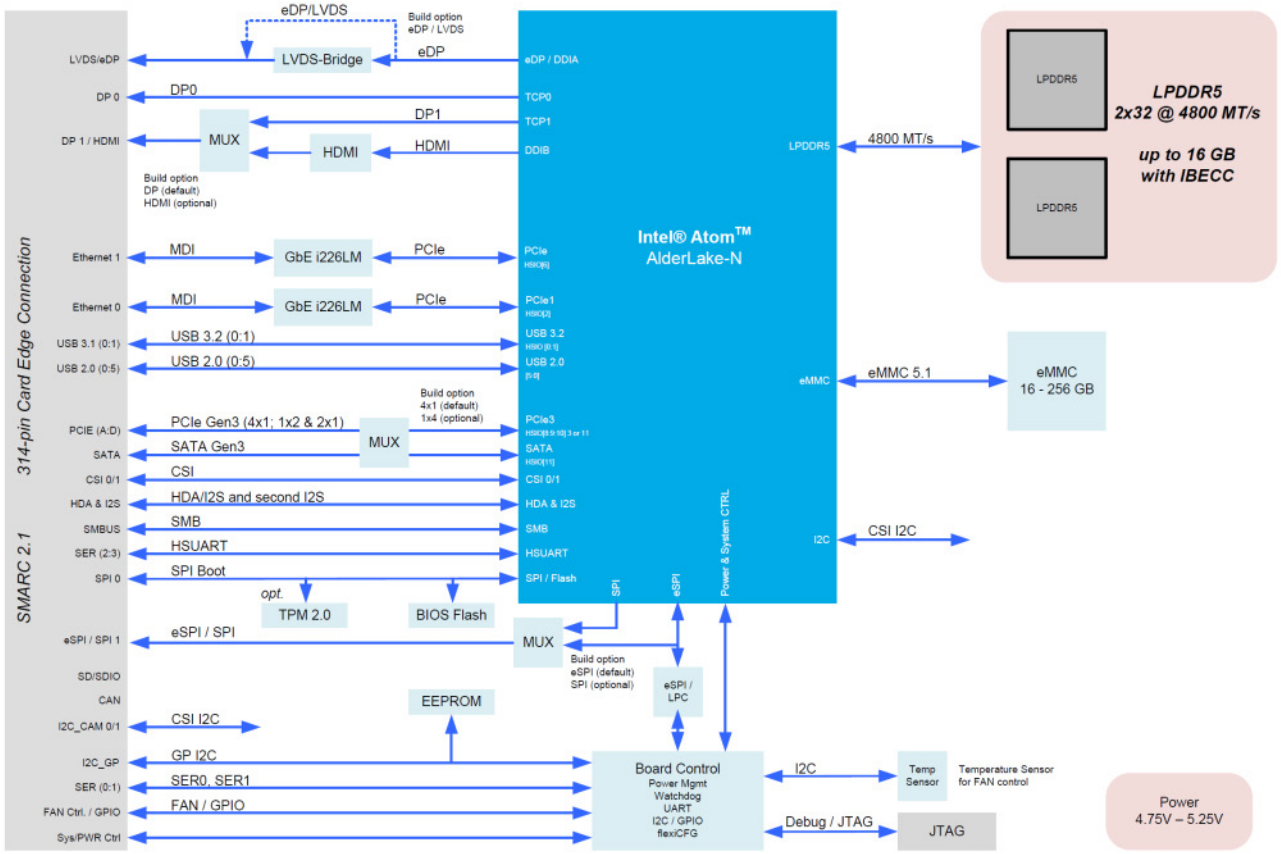

Figure 1: Block Diagram TQMxE41S

3.2 Electrical Characteristics

3.2.1 Supply Voltage

The TQMxE41S supports an input voltage from 4.75 V to 5.25 V.

The following supply voltages are specified at the SMARC connector:

- Main Power Rail: 4.75 V to 5.25 V max input ripple: ±100 mV
- VCC_RTC: 2.0 V to 3.3 V max input ripple: ±20 mV

The input voltages shall rise from 10 % of nominal to 90 % of nominal within 0.1 to 20 ms (0.1 ms ≤ Rise Time ≤ 20 ms).
There must be a smooth and continuous ramp of each DC output voltage from 10 % to 90 % of its final set point within the regulation band.

3.2.2 Power Consumption

The values below show voltage and power consumption details for the TQMxE41S.
The values were measured using the TQMxE41S and the MB-SMARC-3 carrier board.
The measurement was done with two power supplies, one for the TQMxE41S and one for the MB-SMARC-3 carrier board.
The power consumption of each TQMxE41S was measured running Windows® 10, 64 bit and different LPDDR5 configurations. All measurements were done at a temperature of +25 °C and an input voltage of +5.0 V.
The power consumption of the TQMxE41S depends on the application, the mode of operation and the operating system.
The power consumption was measured under the following conditions:

- **Suspend mode:**
  The system is in S5/S4 state, Ethernet ports disconnected.
- **Windows 10, 64 bit, idle:**
  Desktop idle, Ethernet ports disconnected.
- **Windows 10, 64 bit, maximum load:**
  These values show the maximum worst case power consumption, achieved by using the Intel® stress test tool to apply maximum load to the cores only, and cores plus graphics engine
- **Windows 10, 64 bit, Suspend Mode:**
  The system is in S5/S4 state, Ethernet port is disconnected.

The following table shows the power consumption with different CPU configurations.

Table 2: TQMxE41S Power Consumption

Module	Mode		
	Suspend (OS shut down)	Win10, 64 bit idle	Win10, 64 bit max. load
SKU2 N97 with 8GB LPDDR5	0.88 W	4.2 W	15W / 17W
SKU3 N200 with 8GB LPDDR5	0.88 W	4.9 W	8.5W / 16W
SKU4 Core-I3 with 16GB LPDDR5	0.88 W	4.8 W	16W / 18.5 W
SKU5 x7211E with 4GB LPDDR5	0.88 W	5.5 W	8.5W / 12.5W

Note: Power requirement	
	The power supplies on the carrier board for the TQMxE41S must be designed with enough reserve. The carrier board should provide at least twice the maximum workload power of the TQMxE41S. The TQMxE41S supports several low-power states. The power supply of the carrier board has to be stable even with no load.

3.2.2.1 Real Time Clock Power Consumption

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

Table 3: RTC Current Consumption

Integrated RTC	Voltage	Current
Intel® X7000E and Core i3 N-Series "Alder Lake N"	3.0 V	3 µA

The current consumption of the RTC in the Intel® X7000E and Core i3 N-Series "Alder Lake N" in the Product Family Datasheet (Electrical an Thermal Specifications) is specified with 8µA max at room temperature while the system is off. The values measured on was lower than 3µA.

3.3 Environmental conditions

- Operating Temperature Standard: 0 °C to +60 °C
- Storage Temperature: –40 °C to +85 °C
- Relative humidity (operating / storage): 10 % to 90 % (non-condensing)

Attention: Maximum operating temperature	
	Do not operate the TQMxE41S without heat spreader or without heat sink! The heat spreader is not a sufficient heat sink!

3.4 System Components

3.4.1 CPUs

The TQMxE41S supports the Intel® X7000E and Core i3 N-Series.

Table 4: Intel® X7000E Series: Comparison of the SKUs

Mode	Intel® Processor N50	Intel® Processor N97	Intel® Processor N200	Intel® Processor I3-N305		Intel® Processor x7211E	Intel® Processor X7425E	Intel® Processor x7213E
Use Condition	PC-Client					Embedded		
CPU Cores	2	4	4	8		2	4	2
CPU frequency	1.0 GHz	2.0 GHz	1.0 GHz	0.9 GHz	1.8 GHz	1.0 GHz	1.5 GHz	1.7 GHz
Burst frequency	3.4 GHz	3.6 GHz	3.7 GHz	3.8 GHz		3.2 GHz	3.4 GHz	3.2 GHz
UHD Graphics (Execution Units)	16 EUs	24 EUs	32 EUs	32 EUs		16 EUs	24 EUs	16 EUs
Thermal Design Power (TDP)	6 W	12 W	6 W	9 W	15 W	6 W	12 W	10 W

3.4.2 Graphics

The Intel® X7000E Series CPUs includes an integrated Intel® UHD (Gen 12) graphics accelerator. It provides excellent 2D/3D graphics performance with up to three simultaneous display support.

The following list shows some key features of the Intel® X7000E Series CPUs:

- Graphics Technology (Gen 12 Xᵉ LP) with up to 32 Execution Units
- Max. 3 displays @4K60
- Hardware accelerated video decoding/encoding for MPEG2, H.264, WMV9 (VC-1), JPEG/MJPEG, H.265(HEVC), VP9, AV1
- OpenGL 4.6, DirectX 12.1, Vulkan 1.3 support
- OpenCL 3.0 support

The TQMxE41S supports two Digital Display Interface (DDI) and one eDP or LVDS interface at the SMARC connector.

Table 5: Maximum Resolution

Display	Maximum Display Resolution
LVDS	1920 × 1200 at 60 Hz (dual LVDS bus)
eDP	1920x1080@60Hz (for most SKUs)
DP	4096 × 2160 at 60 Hz
HDMI 1.4b	1920 × 1080 at 60 Hz / 3840 x 2160 at 30Hz / 4096 x 2160 @ 24Hz

3.4.3 Memory

3.4.3.1 LPDDR5 SDRAM

The TQMxE41S supports a memory-down 2x32bit LPDDR5 configuration running at up to 4800 MT/s and optional In Band ECC (IBECC). The maximum memory size is 16 Gbyte. The available memory configuration can be either 4 Gbyte, 8 Gbyte, or 16 Gbyte.

3.4.3.2 eMMC

The TQMxE41S supports up to 256 Gbyte on-board eMMC 5.1 flash.

Attention: eMMC OS installation	
	The on-board eMMC Flash requires pre-configuration via EFI Shell before OS installation (e.g. diskpart utility)

3.4.3.3 SPI Boot Flash

The TQMxE41S provides a 256 Mbit SPI boot flash. It includes the uEFI BIOS.
An external SPI boot flash can be used instead of the on-board SPI boot flash.

3.4.3.4 EEPROM

On the TQMxE41S there can be placed a 32 kbit serial EEPROM on the I2C_GP bus. This feature is optional.

3.4.4 Real Time Clock

The TQMxE41S includes a standard RTC integrated in the Intel® X7000E Series CPU.

3.4.5 Trusted Platform Module

The TQMxE41S supports the Trusted Platform Module (TPM) 2.0 (Infineon SLB9670 controller).
Intel® X7000E Series CPU supports also a Firmware Trusted Platform Module (FTPM); this is a Trusted Platform Module 2.0 implementation in firmware. This feature can be configured in the BIOS.

3.4.6 TQ flexible I/O configuration (TQ-flexiCFG)

The module includes a flexible I/O configuration feature, the TQ-flexiCFG.
Using the TQ-flexiCFG feature several I/O interfaces and functions can be configured via a programmable FPGA.
This feature enables the user to integrate special embedded features and configuration options in the TQMxE41S to reduce the carrier board design effort. Here are some examples of the flexible I/O configuration:

- GPIO interrupt configuration
- Interrupt configuration via LPC Serial IRQ
- Serial Port handshake signals via GPIOs
- Integrate additional I/O functions, e.g. additional Serial, I²C, PWM controller or special power management configurations

Please contact support@tq-group.com for further information about the TQ-flexiCFG.

3.5 Interfaces

3.5.1 PCI Express

The TQMxE41S with Intel® X7000E Series CPU supports a very flexible PCI Express configuration with up four PCI Express Gen3 ports.
With a customized BIOS the PCI Express lanes can be configured as follows:

Table 6: PCI Express Configuration Options

SMARC™ Port A – D				Configuration	Configuration
A	B	C	D	4 ports x1 Lane	Configuration in the BIOS (default)
A		C	D	1 Port x2 Lanes + 2 Ports x1 Lane	Configuration via custom BIOS
A		C		1 Port x2 Lanes + 1 Port x2 Lanes	Configuration via custom BIOS and assembly option
A				1 Port x4 Lanes	Configuration via custom BIOS and assembly option

Note: PCIe assembly option	
	With default PCIe assembly option following configurations cannot be used: • 1 Port x2 Lanes + 2 Ports x1 Lane • 1 Port x4 Lanes With the PCIe x4 assembly option SATA port cannot be used.

3.5.2 Serial ATA

The TQMxE41S supports one SATA Gen3.0 interface which supports up to 6 Gb/s. SATA and PCIe form an assembly option. If SATA is used, the following PCIe configurations cannot be used:
1 Port x2 Lanes + 1 Port x2 Lanes
1 Port x4 Lanes

3.5.3 Gigabit Ethernet

The TQMxE41S provides two Intel® i226 Ethernet controller with up to 2.5 Gb/s speed.
In the SMARC specification (1) there are defined two gigabit Ethernet capable ports. Solutions with 2.5 Gb/s are possible with the TQMxE41S. In this case special attention should be paid on the high-speed routing and on the Ethernet Jack or magnetics selection.
When realizing a 1 Gb/s solution, it should be ensured that the established link is limited to this data rate.

3.5.4 Digital Display Interface

The TQMxE41S supports three Display Interfaces at the SMARC connector.
The SMARC Primary Display interface supports either LVDS or eDP as an assembly option.

The SMARC Secondary Display interface (HDMI/DP1) supports DisplayPort or HDMI/DVI with an appropriate level realized on the module.
The SMARC Third Display interface (DP++) supports DisplayPort++ solutions or HDMI/DVI with an appropriate level shifter or retimer on the carrier board.

The TQMxE41S supports the following maximum display resolutions:

- DisplayPort 1.4a up to 4096 × 2304 at 60 Hz
- Embedded DisplayPort 1.4b: Default: up to 1920x1080@60Hz; specific SKU: up to 4096 × 2304 at 60 Hz
- HDMI 1.4b up to 1920 × 1080 at 60 Hz / 3840 x 2160 at 30Hz / 4096 x 2160 @ 24Hz
- HDMI 2.0b (appropriate redriver / retimer on carrier board necessary): 4Kx2K@60Hz

Note: Assembly option for SMARC Secondary Display interface (HDMI/DP1)	
	With default Display assembly option the TQMxE41S provides DP++ on this interface. • Flexible DP++ solutions can be realized on the carrier • HDMI 1.4b or HDMI2.0b solutions are possible by using an appropriate level shifter or redriver or retime on the carrier With the assembly option for HDMI on SMARC Secondary Display interface simple HDMI solutions can be realized on the carrier for SMARC Secondary Display interface: • a special BIOS is necessary to use this option • an example is included in SMARC Design Guide (2) • the HDMI 1.4b capable level shifter on TQMxE41S supports data rates up to 3Gbit/s

Please contact support@tq-group.com for further information about the display configuration.

3.5.5 LVDS Interface

The TQMxE41S supports an LVDS interface which is provided through an on-board eDP to LVDS bridge.
The eDP to LVDS bridge supports single or dual LVDS signalling with colour depths of 18 bits per pixel or 24 bits per pixel up to 112 MHz and a resolution up to 1920 × 1200 @ 60 Hz in dual LVDS mode. The LVDS data packing can be configured either in VESA or JEIDA format.
To support panels without EDID ROM, the eDP to LVDS bridge can emulate EDID ROM behaviour avoiding specific changes in system video BIOS.
Please contact support@tq-group.com for further information about the LVDS configuration.

3.5.6 USB 2.0 Interfaces

The TQMxE41S supports six USB 2.0 and two USB 3.2 Gen2 ports with data rate up to 10 Gb/s at the SMARC connector. The default setting for the USB SuperSpeed ports is 5 Gb/s (USB 3.2 Gen1).
If USB 3.2 Gen2 (10 Gb/s) transfer mode is required, special attention should be paid on the high-speed routing and losses on the SuperSpeed+ signals when designing a carrier.

3.5.7 USB 3.0 Interfaces

The TQMxE41S supports two SuperSpeed+ ports at the SMARC connector.

Note: USB Port Mapping	
	The USB 2.0 port 2 must be paired with USB 3.2 SuperSpeed port 2. The USB 2.0 port 3 must be paired with USB 3.2 SuperSpeed port 3.

3.5.8 General Purpose Input/Output

The TQMxE41S provides 14 GPIO signals at the SMARC connector. These GPIO signals are shared with camera control, fan Control and HD Audio Reset signals. They can be configured by software.

The GPIO signals are integrated in the TQ-flexiCFG block and can be configured flexible. Therefore the signals can also be used for several special functions (see 3.4.6).

Please contact support@tq-group.com for further information about the GPIO configuration and their alternate uses.

3.5.9 Audio Interfaces

The TQMxE41S provides a High Definition Audio (HDA) and an I²S interface, which support Audio codecs at the SMARC connector. The audio codec on the carrier board should be supported by the BIOS of the TQMxE41S. The HDA interface can also be used as second I²S interface.

Please contact support@tq-group.com for further information regarding configuration and supported codecs.

3.5.10 I²C Bus

The TQMxE41S supports a general purpose I²C bus via a dedicated LPC to I²C controller, integrated in the TQ-flexiCFG block. The I²C host controller supports a clock frequency of up to 400 kHz and can be configured independently.

3.5.11 SMBus / Power Management I²C Bus

The TQMxE41S provides an I²C based System Management Bus (SMBus) interface. This bus is also called Power Management I²C Bus.

3.5.12 Serial Peripheral Interface

The TQMxE41S provides an SPI interface. The SPI interface can only be used for SPI boot Flash devices. A second SPI Interface is multiplexed (assembly option) with eSPI Interface.
Please contact support@tq-group.com for further information about eSPI / SPI configuration.

3.5.13 eSPI

The TQMxE41S provides an eSPI interface, which is multiplexed (assembly option) with a second SPI Interface.
Please contact support@tq-group.com for further information about eSPI / SPI configuration.

3.5.14 Serial Ports

The TQMxE41S offers up to four UARTs (Universal Asynchronous Receiver and Transmitter). The register set of SER0 and SER1 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.
SER2 and SER3 are connected to the processor internal UARTs of the Intel® X7000E Series CPU.

3.5.15 Watchdog Timer

The TQMxE41S supports a freely 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 timeout of the watchdog timer ranges from 125 ms to 1 h.
The SMARC specification does not support external hardware triggering of the watchdog. An external watchdog trigger can be configured to GPIO pins at the SMARC connector with the TQ-flexiCFG feature.

3.6 Connectors & LEDs

3.6.1 SMARC Connector

A 314 pin 0.5 mm pitch card edge connector is realized on the TQMxE41S PCB. On the carrier board a connector mechanical compatible to MXM3 graphic cards is used to contact the module. The stacking height is defined by the connector used on the carrier (e.g. 1.5 mm, 2.7 mm, 5 mm, and 8 mm are available).

3.6.2 Debug LED

The TQMxE41S includes a dual colour LED providing boot and BIOS information.
The following table shows some LED boot messages.

Table 7: 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 finished

3.7 SMARC Connector Pinout

This section describes the TQMxE41S SMARC connector pin assignment, which is compliant with the SMARC hardware specification Version 2.1.1.

3.7.1 Signal Assignment Abbreviations

Table 8 lists the abbreviations used in Table 9.

Table 8: Abbreviations used

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

Note: Unused signals on the carrier board	
	If the input signals at the SMARC connector are not used, these signals can be left open on the carrier board, since these signals have a termination on the TQMxE41S.

3.7.2 SMARC Connector Pin Assignment

Table 9: SMARC Connector Pin Assignment

Pin	Pin-Signal	Description	Type	Level	Remark
P1	SMB_ALERT#	SM Bus Alert# (interrupt) signal	I PU	1.8 V	
P2	GND	Ground	GND		
P3	CSI1_CK+	CSI differential clock input	I	LVDS D-PHY	
P4	CSI1_CK–	CSI differential clock input	I	LVDS D-PHY	
P5	GBE1_SDP	IEEE 1588 Trigger Signal	IO	3.3 V	
P6	GBE0_SDP	IEEE 1588 Trigger Signal	IO	3.3 V	
P7	CSI1_RX0+	CSI differential data input	I	LVDS D-PHY	
P8	CSI1_RX0–	CSI differential data input	I	LVDS D-PHY	
P9	GND	Ground	GND		
P10	CSI1_RX1+	CSI differential data input	I	LVDS D-PHY	
P11	CSI1_RX1–	CSI differential data input	I	LVDS D-PHY	
P12	GND	Ground	GND		
P13	CSI1_RX2+	CSI differential data input	I	LVDS D-PHY	
P14	CSI1_RX2–	CSI differential data input	I	LVDS D-PHY	
P15	GND	Ground	GND		
P16	CSI1_RX3+	CSI differential data input	I	LVDS D-PHY	
P17	CSI1_RX3–	CSI differential data input	I	LVDS D-PHY	
P18	GND	Ground	GND		
P19	GBE0_MDI3–	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P20	GBE0_MDI3+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P21	GBE0_LINK100#	Link Speed Indication LED for 100 Mbps	OD	3.3 V tolerant	16mA max
P22	GBE0_LINK1000#	Link Speed Indication LED for 1000 Mbps	OD	3.3 V tolerant	16mA max
P23	GBE0_MDI2–	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P24	GBE0_MDI2+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P25	GBE0_LINK_ACT#	Link / Activity Indication LED	OD	3.3 V tolerant	16mA max
P26	GBE0_MDI1–	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P27	GBE0_MDI1+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P28	GBE0_CTREF	Center-Tap reference voltage for Carrier Ethernet magnetics	PWR		
P29	GBE0_MDI0–	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P30	GBE0_MDI0+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P31	SPI0_CS1#	SPI0 Master Chip Select 1 output	O	1.8 V	
P32	GND	Ground	GND		
P33	SDIO_WP	SD Card: Write Protect	I PU	3.3 V	N/A
P34	SDIO_CMD	SD Card: Command line	IO	3.3 V	N/A
P35	SDIO_CD#	SD Card: Card Detect	I PU	3.3 V	N/A
P36	SDIO_CK	SD Card: Clock	O	3.3 V	N/A
P37	SDIO_PWR_EN	SD Card: Power enable	O	3.3 V	N/A
P38	GND	Ground	GND		
P39	SDIO_D0	SD Card: data path	IO	3.3 V	N/A
P40	SDIO_D1	SD Card: data path	IO	3.3 V	N/A
P41	SDIO_D2	SD Card: data path	IO	3.3 V	N/A
P42	SDIO_D3	SD Card: data path	IO	3.3 V	N/A
P43	SPI0_CS0#	SPI0 Master Chip Select 0 output	O	1.8 V	
P44	SPI0_CK	SPI0 Master Clock output	O	1.8 V	
P45	SPI0_DIN	SPI0 Master Data input (CPU input, SPI device output)	I	1.8 V	
P46	SPI0_DO	SPI0 Master Data output (CPU output, SPI device input)	O	1.8 V	
P47	GND	Ground	GND		
P48	SATA_TX+	Differential SATA transmit data Pair	O	SATA	
P49	SATA_TX–	Differential SATA transmit data Pair	O	SATA	
P50	GND	Ground	GND		
P51	SATA_RX+	Differential SATA receive data Pair	I	SATA	
P52	SATA_RX–	Differential SATA receive data Pair	I	SATA	

3.7.2 SMARC Connector Pin Assignment (continued)

Table 9: SMARC Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Level	Remark
P53	GND	Ground	GND		
P54	ESPI_CS0	ESPI / SPI master chip select	O	1.8 V	
P55	ESPI_CS1#	ESPI master chip select	O	1.8 V	
P56	ESPI_CK	ESPI / SPI master clock output	O	1.8 V	
P57	ESPI_IO_1	ESPI master data I/O / SPI data in	IO	1.8 V	
P58	ESPI_IO_0	ESPI master data I/O / SPI data out	IO	1.8 V	
P59	GND	Ground	GND		
P60	USB0+	USB differential pair	IO	USB	
P61	USB0–	USB differential pair	IO	USB	
P62	USB0_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	(1)
P63	USB0_VBUS_DET	Host power detection (when port is used as device)	I PD	5 V	
P64	USB0_OTG_ID	USB OTG ID input, active high (high ⇨ device)	I PU	3.3 V	
P65	USB1+	USB differential pair	IO	USB	
P66	USB1–	USB differential pair	IO	USB	
P67	USB1_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	(1)
P68	GND	Ground	GND		
P69	USB2+	USB differential pair	IO	USB	
P70	USB2–	USB differential pair	IO	USB	
P71	USB2_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	(1)
P72	RSVD	Reserved			
P73	RSVD	Reserved			
P74	USB3_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	(1)
P75	PCIE_A_RST#	PCIe Port reset output	O	3.3 V	
P76	USB4_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	(1)
P77	PCIE_B_CKREQ#	PCIe Port B clock request (could be pulled low by TQMxE41S)	IO PU	3.3 V	
P78	PCIE_A_CKREQ#	PCIe Port A clock request (could be pulled low by TQMxE41S)	IO PU	3.3 V	
P79	GND	Ground	GND		
P80	PCIE_C_REFCK+	Differential PCIe Link reference clock output	O	PCIe	
P81	PCIE_C_REFCK–	Differential PCIe Link reference clock output	O	PCIe	
P82	GND	Ground	GND		
P83	PCIE_A_REFCK+	Differential PCIe Link reference clock output	O	PCIe	
P84	PCIE_A_REFCK–	Differential PCIe Link reference clock output	O	PCIe	
P85	GND	Ground	GND		
P86	PCIE_A_RX+	Differential PCIe Link receive data pair	I	PCIe	
P87	PCIE_A_RX–	Differential PCIe Link receive data pair	I	PCIe	
P88	GND	Ground	GND		
P89	PCIE_A_TX+	Differential PCIe Link transmit data pair	O	PCIe	
P90	PCIE_A_TX–	Differential PCIe Link transmit data pair	O	PCIe	
P91	GND	Ground	GND		
P92	HDMI_D2+ / DP1_LANE0+	TMDS / HDMI data differential pair / DP data pair	O	DP / HDMI	
P93	HDMI_D2– / DP1_LANE0–	TMDS / HDMI data differential pair / DP data pair	O	DP / HDMI	
P94	GND	Ground	GND		
P95	HDMI_D1+ / DP1_LANE1+	TMDS / HDMI data differential pair / DP data pair	O	DP / HDMI	
P96	HDMI_D1– / DP1_LANE1–	TMDS / HDMI data differential pair / DP data pair	O	DP / HDMI	
P97	GND	Ground	GND		
P98	HDMI_D0+ / DP1_LANE2+	TMDS / HDMI data differential pair / DP data pair	O	DP / HDMI	
P99	HDMI_D0– / DP1_LANE2–	TMDS / HDMI data differential pair / DP data pair	O	DP / HDMI	
P100	GND	Ground	GND		
P101	HDMI_CK+ / DP1_LANE3+	HDMI differential clock output pair / DP data pair	O	DP / HDMI	
P102	HDMI_CK– / DP1_LANE3–	HDMI differential clock output pair / DP data pair	O	DP / HDMI	
P103	GND	Ground	GND		
P104	HDMI_HPD / DP1_HPD	HDMI / DP Hot Plug Detect input	I PD	1.8 V	

1: Configurable through TQ-flexiCFG.

3.7.2 SMARC Connector Pin Assignment (continued)

Table 9: SMARC Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Level	Remark
P105	HDMI_CTRL_CK / DP1_AUX+	HDMI I²C clock / DP AUX Channel	IO	1.8V /3.3 V	
P106	HDMI_CTRL_DAT / DP1_AUX–	HDMI I²C data / DP AUX Channel	IO	1.8V /3.3 V	
P107	DP1_AUX_SEL	DP AUX select (to select between DP and HDMI)	I PD	1.8 V	
P108	GPIO0 / CAM0_PWR#	GPIO / Camera power enable (active low output)	IO PU/O	1.8 V	(2)
P109	GPIO1 / CAM1_PWR#	GPIO / Camera power enable (active low output)	IO PU/O	1.8 V	(2)
P110	GPIO2 / CAM0_RST#	GPIO / Camera reset (active low output)	IO PU/O	1.8 V	(2)
P111	GPIO3 / CAM1_RST#	GPIO / Camera reset (active low output)	IO PU/O	1.8 V	(2)
P112	GPIO4 / HDA_RST#	GPIO / HD audio reset (active low output)	IO PU/O	1.8 V	Preconfigured to HDA_RST# (2)
P113	GPIO5 / PWM_OUT	GPIO / PWM out for fan speed control	IO PU/O	1.8 V	Preconfigured to PWM_OUT (2)
P114	GPIO6 / TACHIN	GPIO / Tachometer input for fan speed measurement	IO PU/O	1.8 V	Preconfigured to TACHIN (2)
P115	GPIO7	GPIO	IO PU	1.8 V	(2)
P116	GPIO8	GPIO	IO PU	1.8 V	(2)
P117	GPIO9	GPIO	IO PU	1.8 V	(2)
P118	GPIO10	GPIO	IO PU	1.8 V	(2)
P119	GPIO11	GPIO	IO PU	1.8 V	(2)
P120	GND	Ground	GND		
P121	I2C_PM_CK	Power management I²C bus: SMBus	IO PU	1.8 V	
P122	I2C_PM_DAT	Power management I²C bus: SMBus	IO PU	1.8 V	
P123	BOOT_SEL0#	Boot source select	I	1.8 V	N/A
P124	BOOT_SEL1#	Boot source select	I	1.8 V	N/A
P125	BOOT_SEL2#	Boot source select (tie to GND to boot from carrier SPI)	I PU	1.8 V	(2)
P126	RESET_OUT#	General purpose reset output to carrier board	O	1.8 V	(2)
P127	RESET_IN#	Reset input from Carrier board	I PU	1.8 V	(2)
P128	POWER_BTN#	Power-button input from Carrier board	I PU	1.8 V	(2)
P129	SER0_TX	Serial port data out	O	1.8 V	(2)
P130	SER0_RX	Serial port data in	I	1.8 V	(2)
P131	SER0_RTS#	Serial port handshake: Request to Send	O	1.8 V	(2)
P132	SER0_CTS#	Serial port handshake: Clear to Send	I	1.8 V	(2)
P133	GND	Ground	GND		
P134	SER1_TX	Serial port data out	O	1.8 V	(2)
P135	SER1_RX	Serial port data in	I	1.8 V	(2)
P136	SER2_TX	Serial port data out	O	1.8 V	
P137	SER2_RX	Serial port data in	I	1.8 V	
P138	SER2_RTS#	Serial port handshake: Request to Send	O	1.8 V	
P139	SER2_CTS#	Serial port handshake: Clear to Send	I	1.8 V	
P140	SER3_TX	Serial port data out	O	1.8 V	
P141	SER3_RX	Serial port data in	I	1.8 V	
P142	GND	Ground	GND		
P143	CAN0_TX	CAN Transmit output	O	1.8 V	N/A
P144	CAN0_RX	CAN Receive input	I	1.8 V	N/A
P145	CAN1_TX	CAN Transmit output	O	1.8 V	N/A
P146	CAN1_RX	CAN Receive input	I	1.8 V	N/A
P147	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P148	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P149	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P150	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P151	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P152	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P153	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P154	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P155	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P156	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	

2: Configurable through TQ-flexiCFG.

3.7.2 SMARC Connector Pin Assignment (continued)

Table 9: SMARC Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Level	Remark
S1	CSI1_TX+ / I2C_CAM1_CK	Camera I²C	IO PU	1.8 V	
S2	CSI1_TX– / I2C_CAM1_DAT	Camera I²C	IO PU	1.8 V	
S3	GND	Ground	GND		
S4	RSVD	Reserved			
S5	CSI0_TX+ / I2C_CAM0_CK	Camera I²C	IO PU	1.8 V	
S6	CAM_MCK	Master clock output for CSI camera support	O	1.8 V	
S7	CSI0_TX– / I2C_CAM0_DAT	Camera I²C	IO PU	1.8 V	
S8	CSI0_CK+	CSI differential clock input	I	LVDS D-PHY	
S9	CSI0_CK–	CSI differential clock input	I	LVDS D-PHY	
S10	GND	Ground	GND		
S11	CSI0_RX0+	CSI differential data input	I	LVDS D-PHY	
S12	CSI0_RX0–	CSI differential data input	I	LVDS D-PHY	
S13	GND	Ground	GND		
S14	CSI0_RX1+	CSI differential data input	I	LVDS D-PHY	
S15	CSI0_RX1–	CSI differential data input	I	LVDS D-PHY	
S16	GND	Ground	GND		
S17	GBE1_MDI0+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S18	GBE1_MDI0–	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S19	GBE1_LINK100#	Link Speed Indication LED for 100 Mbps	OD	3.3 V tolerant	16mA max
S20	GBE1_MDI1+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S21	GBE1_MDI1–	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S22	GBE1_LINK1000#	Link Speed Indication LED for 1000 Mbps	OD	3.3 V tolerant	16mA max
S23	GBE1_MDI2+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S24	GBE1_MDI2–	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S25	GND	Ground	GND		
S26	GBE1_MDI3+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S27	GBE1_MDI3–	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S28	GBE1_CTREF	Center-Tap reference voltage for Carrier Ethernet magnetics	PWR		
S29	PCIE_D_TX+	Differential PCIe Link transmit data pair	O	PCIe	
S30	PCIE_D_TX–	Differential PCIe Link transmit data pair	O	PCIe	
S31	GBE1_LINK_ACT#	Link / Activity Indication LED	OD	3.3 V tolerant	16mA max
S32	PCIE_D_RX+	Differential PCIe Link receive data pair	I	PCIe	
S33	PCIE_D_RX–	Differential PCIe Link receive data pair	I	PCIe	
S34	GND	Ground	GND		
S35	USB4+	USB differential pair	IO	USB	
S36	USB4–	USB differential pair	IO	USB	
S37	USB3_VBUS_DET	Host power detection (when port is used as device)	I PD	5 V	
S38	AUDIO_MCK	I²S: Master clock output to Audio codecs	O	1.8 V	
S39	I2S0_LRCK	I²S: Left& Right audio synchronization clock	IO	1.8 V	
S40	I2S0_SDOUT	I²S: Digital audio Output	O	1.8 V	
S41	I2S0_SDIN	I²S: Digital audio Input	I	1.8 V	
S42	I2S0_CK	I²S: Digital audio clock	IO	1.8 V	
S43	ESPI_ALERT0#	ESPI alert	I PU	1.8 V	
S44	ESPI_ALERT1#	ESPI alert	I PU	1.8 V	N/A
S45	MDIO_CLK	MDIO Signals to Configure Possible PHYs	O	1.8 V	N/A
S46	MDIO_DAT	MDIO Signals to Configure Possible PHYs	IO PU	1.8 V	N/A
S47	GND	Ground	GND		
S48	I2C_GP_CK	General Purpose I²C bus	IO PU	1.8 V	
S49	I2C_GP_DAT	General Purpose I²C bus	IO PU	1.8 V	
S50	HDA_SYNC / I2S2_LRCK	HDA: sync / I²S: Left& Right audio synchronization clock	IO	1.8 V	default: HDA
S51	HDA_SDO / I2S2_SDOUT	HDA: data out / I²S: Digital audio Output	O	1.8 V	default: HDA
S52	HDA_SDI / I2S2_SDIN	HDA: data in / I²S: Digital audio Input	I	1.8 V	default: HDA

3.7.2 SMARC Connector Pin Assignment (continued)

Table 9: SMARC Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Level	Remark
S53	HDA_CK / I2S2_CK	HDA: clock / I²S: Digital audio clock	IO	1.8 V	default: HDA
S54	SATA_ACT#	Active low SATA activity indicator	OD	3.3 V	N/A
S55	USB5_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	(3)
S56	ESPI_IO_2	ESPI master data I/O	IO	1.8 V	
S57	ESPI_IO_3	ESPI master data I/O	IO	1.8 V	
S58	ESPI_RESET#	ESPI Reset	O	1.8 V	
S59	USB5+	USB differential pair	IO	USB	
S60	USB5–	USB differential pair	IO	USB	
S61	GND	Ground	GND		
S62	USB3_SSTX+	Differential USB SuperSpeed transmit data pair	O	USB SS	
S63	USB3_SSTX–	Differential USB SuperSpeed transmit data pair	O	USB SS	
S64	GND	Ground	GND		
S65	USB3_SSRX+	Differential USB SuperSpeed receive data pair	I	USB SS	
S66	USB3_SSRX–	Differential USB SuperSpeed receive data pair	I	USB SS	
S67	GND	Ground	GND		
S68	USB3+	USB differential pair	IO	USB	
S69	USB3–	USB differential pair	IO	USB	
S70	GND	Ground	GND		
S71	USB2_SSTX+	Differential USB SuperSpeed transmit data pair	O	USB SS	
S72	USB2_SSTX–	Differential USB SuperSpeed transmit data pair	O	USB SS	
S73	GND	Ground	GND		
S74	USB2_SSRX+	Differential USB SuperSpeed receive data pair	I	USB SS	
S75	USB2_SSRX–	Differential USB SuperSpeed receive data pair	I	USB SS	
S76	PCIE_B_RST#	PCIe Port reset output	O	3.3 V	
S77	PCIE_C_RST#	PCIe Port reset output	O	3.3 V	
S78	PCIE_C_RX+	Differential PCIe Link receive data pair	I	PCIe	
S79	PCIE_C_RX–	Differential PCIe Link receive data pair	I	PCIe	
S80	GND	Ground	GND		
S81	PCIE_C_TX+	Differential PCIe Link transmit data pair	O	PCIe	
S82	PCIE_C_TX–	Differential PCIe Link transmit data pair	O	PCIe	
S83	GND	Ground	GND		
S84	PCIE_B_REFCK+	Differential PCIe Link reference clock output	O	PCIe	
S85	PCIE_B_REFCK–	Differential PCIe Link reference clock output	O	PCIe	
S86	GND	Ground	GND		
S87	PCIE_B_RX+	Differential PCIe Link receive data pair	I	PCIe	
S88	PCIE_B_RX–	Differential PCIe Link receive data pair	I	PCIe	
S89	GND	Ground	GND		
S90	PCIE_B_TX+	Differential PCIe Link transmit data pair	O	PCIe	
S91	PCIE_B_TX–	Differential PCIe Link transmit data pair	O	PCIe	
S92	GND	Ground	GND		
S93	DP0_LANE0+	DP++ data differential pair	O	DP++	
S94	DP0_LANE0–	DP++ data differential pair	O	DP++	
S95	DP0_AUX_SEL	DP AUX select (to select between DP and HDMI)	I PD	1.8 V	
S96	DP0_LANE1+	DP++ data differential pair	O	DP++	
S97	DP0_LANE1–	DP++ data differential pair	O	DP++	
S98	DP0_HPD	DP++ Hot Plug Detect input	I PD	1.8 V	
S99	DP0_LANE2+	DP++ data differential pair	O	DP++	
S100	DP0_LANE2–	DP++ data differential pair	O	DP++	
S101	GND	Ground	GND		
S102	DP0_LANE3+	DP++ data differential pair	O	DP++	
S103	DP0_LANE3–	DP++ data differential pair	O	DP++	
S104	USB3_OTG_ID	USB OTG ID input, active high (high ⇨ device)	I PU	3.3 V	

3.7.2 SMARC Connector Pin Assignment (continued)

Table 9: SMARC Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Level	Remark
S105	DP0_AUX+	DP++ AUX Channel (could also be used as 3.3 V I²C for HDMI)	IO	DP++ /3.3 V	PU at high AUX_SEL
S106	DP0_AUX–	DP++ AUX Channel (could also be used as 3.3 V I²C for HDMI)	IO	DP++ /3.3 V	PU at high AUX_SEL
S107	LCD1_BKLT_EN	LCD Backlight enable: high enables panel backlight	O	1.8 V	N/A
S108	LVDS1_CK+ / eDP1_AUX+ / DSI1_CLK+	LVDS LCD differential clock pair / eDP AUX Channel	O/IO	LVDS/DP	LVDS only
S109	LVDS1_CK– / eDP1_AUX– / DSI1_CLK–	LVDS LCD differential clock pair / eDP AUX Channel	O/IO	LVDS/DP	LVDS only
S110	GND	Ground	GND		
S111	LVDS1_0+ / eDP1_TX0+ / DSI1_D0+	LVDS / eDP data differential pair	O	LVDS/DP	LVDS only
S112	LVDS1_0– / eDP1_TX0– / DSI1_D0–	LVDS / eDP data differential pair	O	LVDS/DP	LVDS only
S113	eDP1_HPD	eDP Hot Plug Detect	I PD	1.8 V	N/A
S114	LVDS1_1+ / eDP1_TX1+ / DSI1_D1+	LVDS / eDP data differential pair	O	LVDS/DP	LVDS only
S115	LVDS1_1– / eDP1_TX1– / DSI1_D1–	LVDS / eDP data differential pair	O	LVDS/DP	LVDS only
S116	LCD1_VDD_EN	Enable signal for panel power	O	1.8 V	N/A
S117	LVDS1_2+ / eDP1_TX2+ / DSI1_D2+	LVDS / eDP data differential pair	O	LVDS/DP	LVDS only
S118	LVDS1_2– / eDP1_TX2– / DSI1_D2–	LVDS / eDP data differential pair	O	LVDS/DP	LVDS only
S119	GND	Ground	GND		
S120	LVDS1_3+ / eDP1_TX3+ / DSI1_D3+	LVDS / eDP data differential pair	O	LVDS/DP	LVDS only
S121	LVDS1_3– / eDP1_TX3– / DSI1_D3–	LVDS / eDP data differential pair	O	LVDS/DP	LVDS only
S122	LCD1_BKLT_PWM	Display Backlight brightness control output (PWM)	O	1.8 V	N/A
S123	GPIO13	GPIO	IO PU	1.8 V	(3)
S124	GND	Ground	GND		
S125	LVDS0_0+ / eDP0_TX0+ / DSI0_D0+	LVDS / eDP data differential pair	O	LVDS/DP	
S126	LVDS0_0– / eDP0_TX0– / DSI0_D0–	LVDS / eDP data differential pair	O	LVDS/DP	
S127	LCD0_BKLT_EN	LCD Backlight enable: high enables panel backlight	O	1.8 V	
S128	LVDS0_1+ / eDP0_TX1+ / DSI0_D1+	LVDS / eDP data differential pair	O	LVDS/DP	
S129	LVDS0_1– / eDP0_TX1– / DSI0_D1–	LVDS / eDP data differential pair	O	LVDS/DP	
S130	GND	Ground	GND		
S131	LVDS0_2+ / eDP0_TX2+ / DSI0_D2+	LVDS / eDP data differential pair	O	LVDS/DP	
S132	LVDS0_2– / eDP0_TX2– / DSI0_D2–	LVDS / eDP data differential pair	O	LVDS/DP	
S133	LCD0_VDD_EN	Enable signal for panel power	O	1.8 V	
S134	LVDS0_CK+ / eDP0_AUX+ / DSI0_CLK+	LVDS LCD differential clock pair / eDP AUX Channel	O/IO	LVDS/DP	
S135	LVDS0_CK– / eDP0_AUX– / DSI0_CLK–	LVDS LCD differential clock pair / eDP AUX Channel	O/IO	LVDS/DP	
S136	GND	Ground	GND		
S137	LVDS0_3+ / eDP0_TX3+ / DSI0_D3+	LVDS / eDP data differential pair	O	LVDS/DP	
S138	LVDS0_3– / eDP0_TX3– / DSI0_D3–	LVDS / eDP data differential pair	O	LVDS/DP	
S139	I2C_LCD_CK	I²C bus to read display EDID EEPROMs (for LVDS displays)	IO PU	1.8 V	
S140	I2C_LCD_DAT	I²C bus to read display EDID EEPROMs (for LVDS displays)	IO PU	1.8 V	
S141	LCD0_BKLT_PWM	Display Backlight brightness control output (PWM)	O	1.8 V	
S142	GPIO12	GPIO	IO PU	1.8 V	
S143	GND	Ground	GND		(3)
S144	eDP0_HPD	eDP Hot Plug Detect	I PD	1.8 V	
S145	WDT_TIME_OUT#	Watch-Dog-Timer Output	O	1.8 V	(3)
S146	PCIE_WAKE#	PCIe wake up interrupt to host	I PU	3.3 V	(3)
S147	VDD_RTC	Real-time clock circuit-power input	PWR	2 V to 3.3 V	
S148	LID#	Lid open/close indication to module (low: closed lid)	I PU	1.8 V	(3)
S149	SLEEP#	Sleep indicator from carrier board	I PU	1.8 V	(3)
S150	VIN_PWR_BAD#	Power bad indication from Carrier board	I PU	VDD_IN	
S151	CHARGING#	Held low by carrier during battery charging	I PU	1.8 V	(3)
S152	CHARGER_PRSNT#	Held low by carrier if DC input for battery charger is present	I PU	1.8 V	(3)
S153	CARRIER_STBY#	Driven low by module during standby power state	O	1.8 V	(3) (SUS_S3#)
S154	CARRIER_PWR_ON	Signal to carrier to turn on determined power supplies	O	1.8 V	(3)
S155	FORCE_RECOV#	Force recovery input: pull low to load BIOS defaults (edge triggered)	I PU	1.8 V	(3)
S156	BATLOW#	Battery low indication to module	I PU	3.3 V	
S157	TEST#	Held low by carrier for module vendor specific functions	I PU	1.8 V	
S158	GND	Ground	GND		

3: Configurable through TQ-flexiCFG.

4. MECHANICS

4.1 TQMxE41S Dimensions

The dimensions of the TQMxE41S are 82 mm × 50 mm.

Please contact support@tq-group.com for more details about 2D/3D Step models.

4.2 Heat Spreader Dimensions

Heat spreader for the Intel® X7000E Series CPU

- **TQMxE41S-HSP**

TQ-Systems GmbH offers thermal analysis and simulation as a service.
Please contact support@tq-group.com for more details about 2D/3D Step models.

4.3 Mechanical and Thermal Considerations

The TQMxE41S is designed to operate in a wide range of thermal environments.

An important factor for each system integration is the thermal design. The heat spreader acts as a thermal coupling device to the TQMxE41S. Therefore, the heat spreader is thermally coupled with the CPU: It ensures an optimal heat transfer from the TQMxE41S to the heat spreader. The heat spreader itself is not a suitable heat sink!

System designers can implement different passive and active cooling versions through the thermal connection to the heat spreader.

Attention: Thermal Considerations	
	Do not operate the TQMxE41S without heat spreader or without heat sink! The heat spreader is not a sufficient heat sink!

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

Please contact support@tq-group.com for more information about the thermal configuration.

4.4 Protection against external effects

The TQMxE41S itself is not protected against dust, external impact and contact (IP00).

Adequate protection has to be guaranteed by the surrounding system and carrier board.

To support applications in harsh environment, conformal coating can be offered as custom specific add-on.

Please contact support@tq-group.com for further details.

5. SOFTWARE

5.1 System Resources

5.1.1 I²C Bus

The TQMxE41S provides a general purpose I²C port via a dedicated LPC to I²C controller in the TQ-flexiCFG block.
The following table shows the I²C address mapping for the SMARC I²C port.

Table 10: I²C Address Mapping on GP I²C Port

8-bit Address	Function	Remark
0xA0	TQMxE41S EEPROM	–
0xAE	Carrier Board EEPROM	Embedded EEPROM configuration not supported

5.1.2 SMBus

The TQMxE41S provides a System Management Bus (SMBus). On the module there are no SMBus devices.

5.1.3 Memory Map

The TQMxE41S supports the standard PC system memory and I/O memory map.
Please contact support@tq-group.com for further information about the memory map.

5.1.4 IRQ Map

The TQMxE41S supports the standard PC Interrupt routing.
The integrated legacy devices (COM1, COM2) can be configured via the BIOS to different IRQs
Please contact support@tq-group.com for further information about the Interrupt configuration.

5.2 Operating Systems

5.2.1 Supported Operating Systems

The TQMxE41S supports various operating systems:

- Microsoft® Windows® 10
- Linux (i.e. Yocto)

Other operating systems are supported on request.

Please contact support@tq-group.com for further information about supported operating systems.

5.2.2 Driver Download

The TQMxE41S is well supported by standard operating systems, which already include most of the required drivers. The use of the latest Intel® drivers to optimize performance and the full feature set of the TQMxE41S is recommended.

Please contact support@tq-group.com 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 x86 modules.
The TQ-Systems EAPI is compatible with the PICMG® specification.

5.4 Software Tools

Please contact support@tq-group.com for further information about available software tools.

6. BIOS – MENU

The TQMxE41S 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.
For Help Dialog please press <F1>.

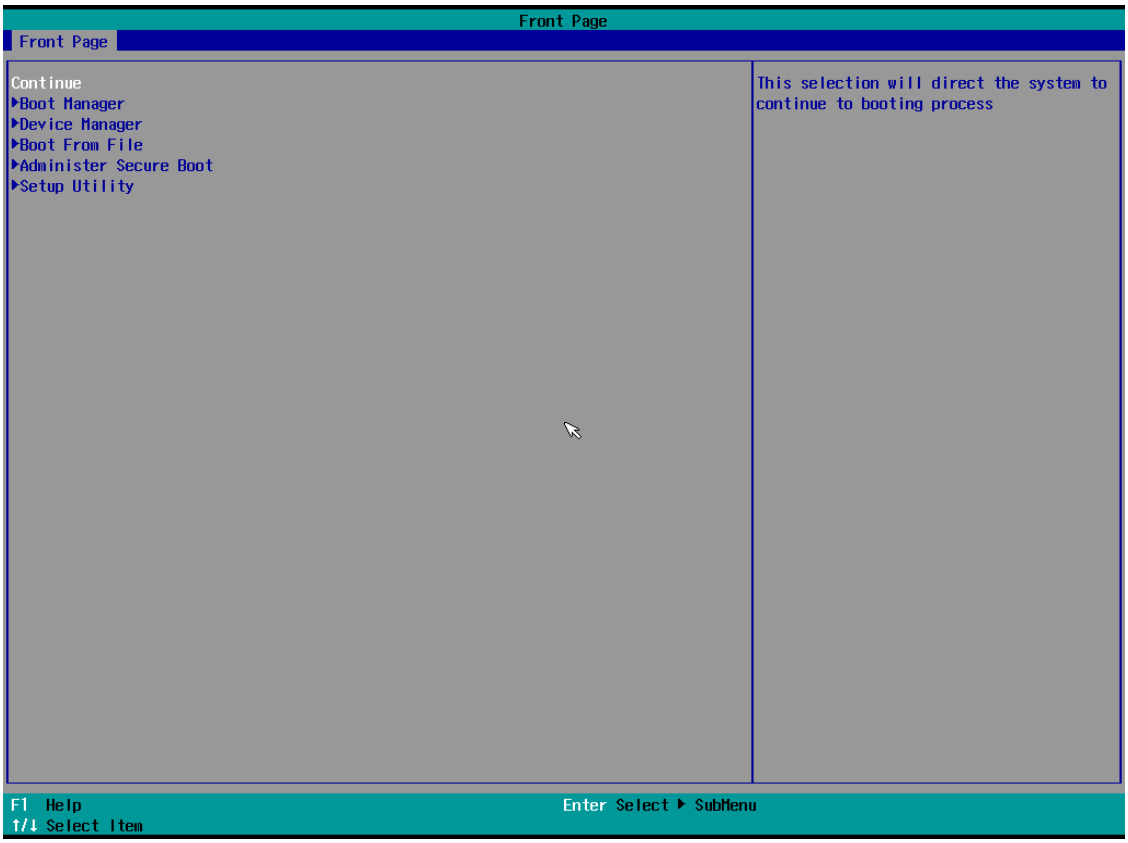

Figure 2: InsydeH2O BIOS Front Page

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 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	
	This option should only be used by advanced users.

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>	In the main screen this buttons allow to change between different languages. Otherwise it allows to change the value of highlighted menu item.
<ENTER>	Press to display or change setup option listed for a certain menu or to display setup sub-screens.
<F9>	Press to load the setup default configuration of the board which cannot be changed by the user. This option has to be confirmed and saved by <F10> afterwards. Leaving the InsydeH2O Setup Utility will discard the changes.
<F10>	Press to save any changes made and exit setup utility by executing a restart.
<ESC>	Press to leave the current screen or sub-screen and discard all changes.

6.6.1 Main

The Main screen shows details regarding the BIOS version, processor type, bus speed, memory configuration and further information. There are three options which 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
SFB Chipset Feature	See submenu	Configure SFB Chipset Feature
RC Advanced Menu	See submenu	Configure RC Advanced Menu Settings
Boot Configuration	See submenu	Configure Boot Settings
USB Configuration	See submenu	Configure the USB supp
Chipset Configuration	See submenu	Advanced Chipset Configuration Options
ACI Table/features Control	See submenu	Configure ACPI Tables/Features Setting
Advanced Platform Information	See submenu	Advanced Platform Information
SIO TQMx86	See submenu	About Super IO Setting
Console Redirection Configuration	See submenu	Console Redirection Settings
H20Uve Configuration	See submenu	Show H20Uve Configuration
H20 Event Log Config Manager	See submenu	Show H20 Event Log Config Manager Utility

6.6.2.1 SFB Chipset Feature

Setup Utility ⇨ Advanced ⇨ SFB Chipset Feature

Menu Item	Option	Description
Logo & SCU Resolution	Auto / 640 x 480 / 800 x 600 / 1024 x 768 / Max Logo Resolution / Max Logo & SCU Resolution	Configuration Logo & Setup Utility Resolution
Rotate Screen	Enabled / Disabled	Enable/Disable Rotate Screen feature, support 90 and 270 degrees clockwise
H20 Setup – IGD display mode	Default / Text Mode / Graphics Mode	Set the setup display mode for IGD
H20 Setup – PEG display mode	Default / Text Mode / Graphics Mode	Set the setup display mode for PEG
GOP eDP/MIPI panel brightness control	Enabled / Disabled	Control GOP eDP/MIPI panel brightness
Graphics Configuration	See submenu	Link to *Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration ⇨ Graphics Configuration*
Wake on USB from S5	Enabled / Disabled	Enable/Disable Wake on USB from S5 state
Force Wake on GPE from S5	Enabled / Disabled	Enable/Disable Force Wake on GPE from S5 state
SATA	See submenu	Link to *Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ SATA Configuration*
eMMC/SD/UFS	See submenu	Link to *Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ SCS Configuration*
NVME(PCIe)	See submenu	Link to *Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ PCI Express Configuration*

6.6.2.2 RC Advanced Menu

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu

Menu Item	Option	Description
ACPI Settings	See submenu	System ACPI Parameters
CPU Configuration	See submenu	CPU Configuration Parameters
Power & Performance	See submenu	Power & Performance Options
Intel(R) Time Coordinated Computing		BIOS Links to Intel(R) Time Coordinated Computing (Intel(R) TCC) relevant options
Memory Configuration	See submenu	Memory Configuration Parameters
System Agent (SA) Configuration	See submenu	System Agent (SA) Parameters
PCH-IO Configuration	See submenu	PCH Parameters
PCH-FW Configuration	See submenu	Configure Management Engine Technology Parameters
ACPI D3Cold Settings	See submenu	ACPI D3Cold related Settings

6.6.2.2.1 ACPI Settings

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
ACPI S3 Support	Enabled / Disabled	Enable ACPI S3 support
Native PCIE Enable	Enabled / Disabled	Bit – PCIe Native * control 0 – ~ Hot Plug 1 – SHPC Native Hot Plug control 2 – ~ Power Management Events 3 – PCIe Advanced Error Reporting control 4 – PCIe Capability Structure control 5 – Latency Tolerance Reporting control
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
D3 Setting for Storage	Disabled / D3Hot	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 enabled, it also disable 8254 timer for SLP_S0 support.
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

6.6.2.2.2 CPU Configuration

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ CPU Configuration

Menu Item	Option	Description
C6DRAM	Enabled / Disabled	Enable/Disable moving of DRAM contents to PRM memory when CPU is in C6 state
CPU Flex Ratio Override	Enabled / Disabled	Enable/Disable CPU Flex Ratio Programming
CPU Flex Ratio Settings	[X]	This Value must be between Max Efficiency Ratio (LFM) and Maximum non-turbo ratio set by Hardware (HFM)
Hardware Prefetcher	Enabled / Disabled	To turn on/off the MLC streamer prefetcher
Adjacent Cache Line Prefetch	Enabled / Disabled	To turn on/off prefetching of adjacent cache lines
Intel (VMX) Virtualization Technology	Enabled / Disabled	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanerdpool Technology.
PECI	Enabled / Disabled	Enable/Disable PECI
AVX	Enabled / Disabled	Enable/Disable the Avx 2 Instructions. This is applicable for Performance-core only
Active Efficient-cores	All / 1	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.
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 MachineCheck
MonitorMWait	Enabled / Disabled	Enable/Disable MonitorMWait, if Disable MonitorMWait, the AP threads Idle Manner should not set in MWait Loop
CPU SMM Enhancement	See submenu	CPU SMM Enhancement

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ CPU Configuration ⇨ CPU SMM Enhancement

Menu Item	Option	Description
SMM Use Delay Indication	Enabled / Disabled	Enable/Disable usage of SMM_DELAYED MSR for MP sync in SMI
SMM Use Block Indication	Enabled / Disabled	Enable/Disable usage of SMM_BLOCKED MSR for MP sync in SMI
SMM Use SMM en-US Indication	Enabled / Disabled	Enable/Disable usage of SMM_ENABLE MSR for MP sync in SMI

6.6.2.2.3 Power & Performance

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ Power & Performance

Menu Item	Option	Description
CPU – Power Management Control	See submenu	CPU – Power Management Control Options
GT – Power Management Control	See submenu	CPU – Power Management Control Options
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 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. (RTH is controlled through MSR 1FC bit 20)
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.
EPB override over PECI	Enabled / Disabled	Enable/Disable EPB override over PECI. Enable by sending pcode command 0x2b, subcommand 0x3 to 1. This will allow 00B EPB PECI override control.
HwP Lock	Enabled / Disabled	Enable/Disable HWP Lock support in Misc Power Management MSR.
HDC Control	Enabled / Disabled	This option allows HDC configuration. Disabled: Disable HDC Enabled: Can be enabled by OS if OS native support is available.
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.
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.
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 / C3 / C1 and C3	Configure C-State Auto Demotion. This option will be hidden if C states is Disabled.
C-State Un-demotion	Disabled / C1 / C3 / C1 and C3	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.

Menu Item	Options	Description
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 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.
Custom P-state Table	See submenu	Add Custom P-state Table
EC Turbo Control Mode	Enabled / Disabled	Enable/Disable EC Turbo Control mode
Energy Performance Gain	Enabled / Disabled	Enable/Disable Energy Performance Gain
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 6 ECX[3] will read 0 indicating no support for Energy Efficient policy setting. When set to 1 will enable access to ENRGY_PERFORMANCE_BIAS MSR 1B0h and CPUID Function 6 ECX[3] will read 1 indicating 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.
Power Limit 1 Override	Enabled / Disabled	Enable/Disable Power Limit 1 override. If this option is disabled, BIOS will program the default values for Power Limit 1 and Power Limit 1 Time Window.
Power Limit 2 Override	Enabled / Disabled	Enable/Disable Power Limit 2 override. If this option is disabled, BIOS will program the default values for Power Limit 1 and Power Limit 2 Time Window.
Power Limit 2	[X]	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8 W when programming. If the value is 0, BIOS will program this value as 1,25*Processor Base Power (TDP). For 12.50 W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Energy Efficient Turbo	Enabled / Disabled	Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overclocking situations where turbo frequency must remain constant. Otherwise, leave enabled.

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 a 125W, enter 1000). For ATX12V0 Percent, Range is 0-1600 (ex. For 200%, enter 1600). Uses BIOS VR mailbox command 0xB.
Min Voltage Override	Enabled / Disabled	Min Voltage Override. Enable to override minimum voltage for runtime and for C8.
VccIn Aux Icc Max	[X]	Sets the Max Icc VccIn Aux value defined in 1/4A increments. Range is 0-512. For an IccMax 32A, enter 128(32*4).
VccIn Aux IMON Slope	[X]	VccIn Aux IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0=Auto. Uses BIOS VR mailbox command 0x18.
VccIn Aux IMON Offset	[X]	VccIn Aux IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON uses BIOS VR mailbox command 0x18.
VccIn Aux IMON prefix	+ / -	Sets the offset value as positive or negative.
Vsys/Psys Critical	Disabled / Psys Critical / Vsys Critical	Vsys/Psysy 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 Mantissa 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)
VR Power Delivery Design	AUTO / ADL P X	Specifies the ADL Desktop board design used for the VR settings override values. By default, BIOS will override the default Desktop VR settings based on the board design. A value of AUTO(0) will use the board ID to determine the board design. Any other value will override the board id logic to provide a custom VR Power Delivery Design value. This is intended primarily for validation.
Acoustic Noise Settings	See submenu	Configure Acoustic Noise Settings for IA, GT and SA domains
Core/IA VR Settings	See submenu	Core/IA VR settings
GT VR Settings	See submenu	GT 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 Periodicity 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 Periodicity Alteration (DPA) tuning.
Ramp Up Down Time	[X]	Set the maximum Ramp Up Down randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
Disable Fast PKG C State Ramp for IA 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 IA Domain	Fast/2 / Fast/4 / Fast/8 / Fast/16	Set VR IA Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number. The number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise.
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 State ramp time; Slow slew rate equals to Fast divided by number. The number is 2, 4, 8 to slow down the slew rate to help minimize acoustic noise divide by 16 is disabled.

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

Menu Item	Options	Description
VR Config Enable	Enabled / Disabled	VR Config Enable
AC Loadline	[X]	AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). = AUTO/HW default. Uses BIOS mailbox command 0x2.
DC Loadline	[X]	DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). = AUTO/HW default. Uses BIOS mailbox command 0x2.
PS Current Threshold1	[X]	PS Current Threshold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS Current Threshold2	[X]	PS Current Threshold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS Current Threshold3	[X]	PS Current Threshold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS3 Enable	Enabled / Disabled	PS3 Enable/Disable. 0 – Disabled, 1 – Enabled. Uses BIOS VR mailbox command 0x3
PS4 Enable	Enabled / Disabled	PS4 Enable/Disable. 0 – Disabled, 1 – Enabled. Uses BIOS VR mailbox command 0x3

Menu Item	Options	Description
IMON Slope	[X]	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4.
IMON Offset	[X]	IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON uses BIOS VR mailbox command 0x4.
IMON Prefix	+ / -	Sets the offset value as positive or negative.
VR Current Limit	[X]	Voltage Regulator Current Limit (IccMax). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. A value uf 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6.
VR Voltage Limit	[X]	Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 – 7999mV. Uses BIOS VR mailbox command 0x8.
TDC Enable	Enabled / Disabled	TDC Enable. 0 – Disable, 1 - Enable
TDC Current Limit	[X]	TDC Current Limit, defined in 1/8 increments. Range is 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A.
TDC Time Window	[X]	VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s.
TDC Lock	Enabled / Disabled	TDC Lock
IRMS	Enabled / Disabled	Enable/Disable IRMS – Current root mean squar

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

Menu Item	Options	Description
VR Config Enable	Enabled / Disabled	VR Config Enable
AC Loadline	[X]	AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). = AUTO/HW default. Uses BIOS mailbox command 0x2.
DC Loadline	[X]	DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). = AUTO/HW default. Uses BIOS mailbox command 0x2.
PS Current Threshold1	[X]	PS Current Threshold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS Current Threshold2	[X]	PS Current Threshold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS Current Threshold3	[X]	PS Current Threshold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS3 Enable	Enabled / Disabled	PS3 Enable/Disable. 0 – Disabled, 1 – Enabled. Uses BIOS VR mailbox command 0x3
PS4 Enable	Enabled / Disabled	PS4 Enable/Disable. 0 – Disabled, 1 – Enabled. Uses BIOS VR mailbox command 0x3
IMON Slope	[X]	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4.
IMON Offset	[X]	IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON uses BIOS VR mailbox command 0x4.
IMON Prefix	+ / -	Sets the offset value as positive or negative.
VR Current Limit	[X]	Voltage Regulator Current Limit (IccMax). This value represents the Maximum instantaneous current allowed at any given time. The value

Menu Item	Options	Description
		is represented in 1/4 A increments. A value uf 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6.
VR Voltage Limit	[X]	Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 – 7999mV. Uses BIOS VR mailbox command 0x8.
TDC Enable	Enabled / Disabled	TDC Enable. 0 – Disable, 1 - Enable
TDC Current Limit	[X]	TDC Current Limit, defined in 1/8 increments. Range is 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A.
TDC Time Window	[X]	VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s.
TDC Lock	Enabled / Disabled	TDC Lock

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

Menu Item	Options	Description
RFI Frequency	[X]	Set desired RFI frequency, in increments of 100KHz. (For a frequency of 100,6MHz, enter 1006.)
FIVR Spread Spectrum	Enabled / Disabled	Enable or Disable the FIVR Spread Spectrum
RFI Spread Spectrum	[X]	Set the Spread Spectrum

Setup Utility ⇨ Advanced ⇨ Power & Performance ⇨ CPU – Power Management Control ⇨ Custom P-state Table

Menu Item	Options	Description
Number of P states	[X]	Sets the number of custom P-states. At least 2 states must be present.

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. BIOS will round to the nearest 1/8W when programming. For 12.5W, enter 12500. XE SKU: Any value can be programmed. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP Limit. If value is 0, BIOS leaves the hardware default value.
Power Limit 3 Time Window	[X]	Power Limit 3 Time Window value in Milli seconds. The value may vary 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
Power Limit 3 Lock	Enabled / Disabled	Power Limit 3 MSR 615h 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 0xE2[15], CFG Lock bit
Overlocking Lock	Enabled / Disabled	Enable/Disable Overlocking Lock (BIT 20) in FLEX_RATIO(194) MSR

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

Menu Item	Options	Description
RC6 (Render Standby)	Enabled / Disabled	Check to enable render standby support.
Maximum GT frequency	Default Max Frequency / 100 – 1200 MHz	Maximum GT frequency limited by the user. Choose between 200 MHz (RPM) and 1000 MHz (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.

6.6.2.2.4 Memory Configuration

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ Memory Configuration

Menu Item	Option	Description
Safe Mode Support	Enabled / Disabled	Safe Mode enable support. Option will be used for changes/Was that may affect an stable MRC.
SA GV	Enabled / Disabled / Fixed to 1st Point / Fixed to 2nd Point / Fixed to 3rd Point / Fixed to 4th Point	System Agent Geyserville. Can disable, fix to a specific point, or enable 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	[X]	Gear ratio for this SAGV point. 0-Auto. 1-G1, 2-G2, 4-G4.
Second Point Frequency	[X]	Specify the frequency for the given point. 0 – MRC auto. Else a specific frequency as an integer: 1333
Second Point Gear	[X]	Gear ratio for this SAGV point. 0-Auto. 1-G1, 2-G2, 4-G4.
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	[X]	Gear ratio for this SAGV point. 0-Auto. 1-G1, 2-G2, 4-G4.
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	[X]	Gear ratio for this SAGV point. 0-Auto. 1-G1, 2-G2, 4-G4.
Row Hammer Mode	Disabled / FRM / pTRR	Row Hammer Prevention Mode. RFM will fall back to pTRR if not available.
RH LFSR0 Mask	[X]	LFSR0 mask for RH pTRR.
RH LFSR1 Mask	[X]	LFSR1 mask for RH pTRR.
MC Refresh Rate	NORMAL Refresh / 1x Refresh 2x Refresh / 4x Refresh	Select refresh rate on the MC.
Refresh Watermarks	High / Low	Sets Refresh Panic Watermark and Refresh High Priority Watermark to HIGH or LOW values.
Per Bank Refresh	Enabled / Disabled	Enables and Disables the per bank refresh. This only impacts memory technologies that support PBR: LPDDR4, LPDDR5 and DDR5.
Memory Scrambler	Enabled / Disabled	Enable/Disable Memory Scrambler Support.

Menu Item	Option	Description
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.

6.6.2.2.5 System Agent (SA) Configuration

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ System Agent (SA) Configuration

Menu Item	Options	Description
Graphics Configuration	See submenu	Graphics Configuration
TCSS setup menu	See submenu	TCSS Configuration settings
PCI Express Configuration	See submenu	PCI Express Configuration settings
Stop Grant Configuration	Auto / Manual	Automatic/Manual stop grant configuration
VT-d	Enabled / Disabled	VT-d capability.
Control Iommu Pre-boot Behavior	Enabled / Disabled	Enable IOMMU in Pre-boot environment (if DMAR table is installed in DXE and if VTD_INFO_PPI is installed in PEI.)
X2APIC Opt Out	Enabled / Disabled	Enable or Disable X2APIC_OPT_OUT bit.
DMA Control Guarantee	Enabled / Disabled	Enable or Disable DMA_CONTROL_GUARANTEE bit.
Thermal Device (B0:D4:F0)	Enabled / Disabled	Enable or Disable SA Thermal Device. Always enabled for ICL A0 stepping.
Cpu CrashLog (Device 10)	Enabled / Disabled	Enable or Disable Cpu CrashLog Device.
GNA Device (B0:D8:F0)	Enabled / Disabled	Enable or Disable SA GNA Device.
CRID Support	Enabled / Disabled	Enable or Disable SA CRID and TCSS CRID control for Intel SIPP.
WRC Feature	Enabled / Disabled	Enable or Disable SA WRC(Write Cache) Feature of IOP. When enabled, supports IO devices allocating onto the ring and into LLC.
Above 4 GB MMIO BIOS assignment	Enabled / Disabled	Enable or Disable above 4 GB MemoryMappedIO BIOS assignment. This is enabled automatically when Aperture Size is set to 2048 MB.
IPU Device (B0:D5:F0)	Enabled / Disabled	Enable/Disable SA IPU Device
IPU 1181 Dash Camera	Enabled / Disabled	Enable/Disable SA 1181 IPU Dash Camera support.

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

Menu Item	Option	Description
Graphics Turbo IMON Current	[X]	Graphics turbo IMON current values supported (14 – 31)
Skip Scanning of External Gfx Card	Enabled / Disabled	If enabled, it will not scan for External Gfx Card on PEG and PCH PCIE Ports.
Dual Vga Controllers Support	Enabled / Disabled	Dual Vga Controllers Support on UEFI Boot Type
Primary Display	Auto / IGFX / PCH PCI	Select which of IGFX/PEG/PCI Graphics device should be Primary Display or select HG for Hybrid Gfx.
Internal Graphics	Auto / Enabled / Disabled	Keep IGFX enabled based on the setup options.
GTT Size	2MB / 4MB / 8MB	Select the GTT Size.
Aperture Size	128MB / 256MB / 512MB / 1024MB	Select the Aperture Size. Note: Above 4 GB MMIO BIOS assignment is automatically enabled when selecting 2048 MB aperture. To use this feature, please disable CSM support.
PSMI SUPPORT	Enabled / Disabled	PSMI Enable/Disable

Menu Item	Option	Description
DVMT Pre-Allocated	[X]	Select DVMT5.0 (Dynamic Video Memory Technology) Pre-Allocated (fixed) Graphics Memory size used by the Internal Graphic Device.
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.
RC1p Support	Enabled / Disabled	Enable/Disable RC1p support. If RC1p is enabled, send a RC1p frequency request to PMA based other conditions being met.
PAVP Enable	Enabled / Disabled	Enable/Disable PAVP.
Cdynmax Clamping Enable	Enabled / Disabled	Enable/Disable Cdynmax Clamping.
Cd Clock Frequency	192 MHz / 307.2 MHz / 556.8 MHz / 652.8 MHz / Max CdClock freq basen on Reference Clk	Select the highest Cd Clock frequency supported by the platform.
VBT Select	eDP / MIPI / DP (DDIA) & HDMI (DDIB) / ADLN_DDR4_RVP	Select VBT for GOP Driver Select Vbt to MIPI if any of the Display has MIPI
Enable Display Audio Link in Pre-OS	Enabled / Disabled	Enable: Display Audio Link will be enabled in Pre-OS. Disabled: Display Audio Link will be disabled in Pre-OS
IUER Button Enable	Enabled / Disabled	Enable/Disable IUER Button Functionality
LCD Control	See submenu	LCD Control
Intel® Ultrabook Event Support	See submenu	LCD Control

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ System Agent (SA) Configuration ⇨ Graphics Configuration ⇨ LCD Control

Menu Item	Option	Description
Primary IGFX Boot Display	VBIOS Default / EFP / LFP / EFP3 / EFP2 / EFP4	Select the Video Device which will be activated during POST. This has no effect if external graphics present. Secondary boot display selection will appear based on your selection. VGA modes will be supported only on primary display
LCD Panel Type	[X]	Select LCD panel used by Internal Graphics Device by selecting the appropriate setup item.
Panel Scaling	Auto / Off / Force Scaling	Select the LCD panel scaling option used by the Internal Graphics Device.
Backlight Control	PWM Inverted / PWM Normal	Backlight Control Setting
Active LFP	No eDP / eDP Port-A	Select the Active LFP Configuration. No LVDS: VBIOS does not enable LVDS. Int-LVDS: VBIOS enables LVDS driver by Integrated encoder. SDVO LVDS: VBIOS enables LVDS driver by SDVO encoder. eDP Port-A: LFP Driven by Int-DisplayPort encoder from Port-A. eDP Port-D: LFP Driven by Int-DisplayPort encoder from Port-D (through PCH).
Panel Color Depth	18Bit / 24 Bit	Select the LFP Panel Color Depth
Backlight Brightness	[X]	Set VBIOS Brightness. Range: 0-255.

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ System Agent (SA) Configuration ⇨ Graphics Configuration ⇨ Intel® Ultrabook Event Support

Menu Item	Option	Description
IUER Slate Enable	Enabled / Disabled	Enable/Disable IUER Slate Functionality
IUER Dock Enable	Enabled / Disabled	Enable/Disable IUER Dock Functionality

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

Menu Item	Option	Description
TCSS xHCI Support	Enabled / Disabled	Enable / Disable TCSS xHCI.

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ System Agent (SA) Configuration ⇨ PCI Express Configuration

Menu Item	Option	Description
Fia Programming	Enabled / Disabled	Load Fia Configuration if Enabled for each root port.
Compliance Test Mode	Enabled / Disabled	Enable when using Compliance Load Board.
CDR Relock	Enabled / Disabled	Enable/Disable CDR Relock.
Assertion on Link Down GPIOs	Enabled / Disabled	GPIO Assertion on Link Down
PCI Express Slot Selection	M2 slot / CEMx4 slot	Select the PCIe M2 or CEMx4 slot
PCIE Resizable BAR Support	Auto / Enabled / Disabled	Enable/Disable PCIE Resizable BAR Support.
PCI Express Root Port 1	See submenu	PCI Express Root Port Settings. PCIe Root Port 1-2 = USB 3.2. PCIe Root Port 3 = OnBoard Ethernet i226. PCIe Root Port 4 = PCIe SMARC Port D. PCIe Root Port 7 = OnBoard Ethernet i226. PCIe Root Port 9/10/11 = PCIe SMARC Port A/B/C. PCIe Root Port 12 = SATA 1 Port
PCI Express Root Port 2	See submenu	PCI Express Root Port Settings. PCIe Root Port 1-2 = USB 3.2. PCIe Root Port 3 = OnBoard Ethernet i226. PCIe Root Port 4 = PCIe SMARC Port D. PCIe Root Port 7 = OnBoard Ethernet i226. PCIe Root Port 9/10/11 = PCIe SMARC Port A/B/C. PCIe Root Port 12 = SATA 1 Port
PCI Express Root Port 3	See submenu	PCI Express Root Port Settings. PCIe Root Port 1-2 = USB 3.2. PCIe Root Port 3 = OnBoard Ethernet i226. PCIe Root Port 4 = PCIe SMARC Port D. PCIe Root Port 7 = OnBoard Ethernet i226. PCIe Root Port 9/10/11 = PCIe SMARC Port A/B/C. PCIe Root Port 12 = SATA 1 Port

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ System Agent (SA) Configuration ⇨ PCI Express Configuration ⇨ PCI 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.
PCI Express Clock Gating	Enabled / Disabled	PCI Express Clock Gating Enable/Disable for each root port.
PCI Express Power Gating	Enabled / Disabled	PCI Express Power Gating Enable/Disable for each root port.
ASPM	Disabled / L1 / Auto	PCI Express Active State Power Management settings.
Gen3 Eq Phase3 Method	Hardware / Static Coeff.	PCIe Gen3 Equalization Phase 3 Method
Gen4 Eq Phase3 Method	Hardware / Static Coeff.	PCIe Gen3 Equalization Phase 3 Method
ACS	Enabled / Disabled	Enable or Disable Access Control Services extended capability.
PTM	Enabled / Disabled	Enable or Disable Precision Time Measurement.
DPC	Enabled / Disabled	Enable or Disable Downstream Port Containment.
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
Multi-VC	Enabled / Disabled	Enabled / Disabled Multi Virtual Channel
EDPC	Enabled / Disabled	Enable or Disable Rootport extensions for Downstream Port Containment.

Menu Item	Options	Description
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.
CT0	Enabled / Disabled	PCI Express Completion Timer T0 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.
Advanced Error Reporting	Enabled / Disabled	Advanced Error Reporting enable/disable.
PCIe Speed	Auto / Gen1 / Gen2 / Gen3	Configure PCIe Speed.
Enable ClockReq Messaging	Enabled / Disabled	Enable or Disable ClockReq Messaging
Transmitter Half Swing	Enabled / Disabled	Transmitter Half Swing Enable/Disable
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.
P2P Support	Enabled / Disabled	Program P2P Support Registers according to setup option
CPU PCIE Func0 Link Disable	Enabled / Disabled	CPU PCIE Func0 Disable while Device attached into Port having Func0 and FuncN
LTR	Enabled / Disabled	PCH PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Auto / Manual / Disabled	Snoop Latency Override for SA 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 SA PCIE. Disabled: Disable override Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Force LTR Override	Enabled / Disabled	Force LTR Override for SA 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
UPTP	[X]	Upstream Port Transmitter Preset.
DPTP	[X]	Downstream Port Transmitter Preset
UPTP	[X]	Upstream Port Transmitter Preset.
DPTP	[X]	Downstream Port Transmitter Preset

6.6.2.2.6 PCH-IO Configuration

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-IO Configuration

Menu Item	Options	Description
PCI Express Configuration	See submenu	PCI Express Configuration settings.
SATA Configuration	See submenu	SATA Device Options settings.
USB Configuration	See submenu	USB Configuration settings.
Security Configuration	See submenu	
HD Audio Configuration	See submenu	HD Audio Subsystem Configuration Settings.
Seriallo Configuration	See submenu	HD Audio Subsystem Configuration settings.

Menu Item	Options	Description
SCS Configuration	See submenu	Storage and Communication Subsystem (SCS) Configuration
Skip VCCIN_AUX Configuration	Enabled / Disabled	Skips VCCIN_AUX Configuration if enabled
Foxville I225 LAN Controller	Enabled / Disabled	Enable/Disable Foxville I225 LAN Controller.
EFI Network	Onboard NIC / 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).
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
TCO Timer WDAT Table	Not Present / Present and Enabled / Present and Disabled	Enable/Disable TCO Timer WDAT Table
Pcie Ref Pll SSC	Auto / X% / Disabled	Pcie Ref Pll SSC Percentage. Auto – Keep hw default, no BIOS override Range is 0.0% - 0.5%
IOAPIC 24-119 Entries	Enabled / Disabled	Enables/Disables IOAPIC 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)
HOST_C10 reporting to Target	Enabled / Disabled	This option enables HOST_C10 reporting to Target via eSPI Virtual Wire.
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

PCI Express Configuration

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-IO Configuration ⇨ PCI Express Configuration

Menu Item	Option	Description
DMI Link ASPM Control	Disabled / L0s / L1 / L0xL1 / Auto	The control of Active State Power Management of the DMI Link.
Porth8xh Decode	Enabled / Disabled	PCI Express Porth8xh Decode Enable/Disable.
Compliance Test Mode	Enabled / Disabled	Enable when using Compliance Load Board.
PCIe function swap	Enabled / Disabled	When disabled, prevents PCIE rootport function swap. If any function other than 0th is enabled, 0th will become visible.
PCIe EQ settings	See submenu	This form contains options for controlling PCIe EQ process.
PCI Express Root Port X	See submenu	PCI Express Root Port Settings. PCIe Root Port 1-2 = USB 3.2. PCIe Root Port 3 = OnBoard Ethernet i226. PCIe Root Port 4 = PCIe SMARC Port D. PCIe Root Port 7 = OnBoard Ethernet i226. PCIe Root Port 9/10/11 = PCIe SMARC Port A/B/C. PCIe Root Port 12 = SATA 1 Port
PCIE clocks	See submenu	PCIE clocks

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-IO Configuration ⇨ PCI Express Configuration ⇨ 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.

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-IO Configuration ⇨ PCI Express Configuration ⇨ PCI 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 / L1 / Auto	PCI Express Active State Power Management settings.
L1 Substates	Disabled / L1.1 / L1.1 & L1.2	PCI Express L1 Substates settings.
L1 Low	Enabled / Disabled	PCI Express L1 Low Substate Enable/Disbale
ACS	Enabled / Disabled	Enable or Disable Access Control Services extended capability.
PTM	Enabled / Disabled	Enable or Disable Precision Time Measurement.
DPC	Enabled / Disabled	Enable or Disable Downstream Port Containment.
EDPC	Enabled / Disabled	Enable or Disable Rootport extensions for Downstream Port Containment.
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.
Advanced Error Reporting	Enabled / Disabled	Advanced Error Reporting enable/disable.
PCIe Speed	Auto / Gen1 / Gen2 / Gen3	Configure PCIe Speed.
Transmitter Half Swing	Enabled / Disabled	Transmitter Half Swing Enable/Disable
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.
Extra Bus Reserved	[X]	Extra Bus Reserved (0-7) for bridges behind this Root Bridge.
Reserved Memory	[X]	Reserved Memory for this Root Bridge (1-20) MB
Reserved I/O	[X]	Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge
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.

Menu Item	Options	Description
LTR Lock	Enabled / Disabled	PCIE LTR Configuration Lock
Peer Memory Write Enable	Enabled / Disabled	Peer Memory Write Enable/Disable

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-IO Configuration ⇨ PCI Express Configuration ⇨ PCIE clocks

Menu Item	Options	Description
Clock0 assignment	Platform-POR / Enabled / Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabledeven if unused. Disabled = Disable clock.
ClkReq for Clock0	Platform-POR / Enabled / Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock1 assignment	Platform-POR / Enabled / Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabledeven if unused. Disabled = Disable clock.
ClkReq for Clock1	Platform-POR / Enabled / Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock2 assignment	Platform-POR / Enabled / Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabledeven if unused. Disabled = Disable clock.
ClkReq for Clock2	Platform-POR / Enabled / Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock3 assignment	Platform-POR / Enabled / Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabledeven if unused. Disabled = Disable clock.
ClkReq for Clock3	Platform-POR / Enabled / Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock4 assignment	Platform-POR / Enabled / Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabledeven if unused. Disabled = Disable clock.
ClkReq for Clock4	Platform-POR / Enabled / Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock5 assignment	Platform-POR / Enabled / Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabledeven if unused. Disabled = Disable clock.
ClkReq for Clock5	Platform-POR / Enabled / Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock6 assignment	Platform-POR / Enabled / Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabledeven if unused. Disabled = Disable clock.
ClkReq for Clock6	Platform-POR / Enabled / Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock7 assignment	Platform-POR / Enabled / Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabledeven if unused. Disabled = Disable clock.
ClkReq for Clock7	Platform-POR / Enabled / Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock8 assignment	Platform-POR / Enabled / Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabledeven if unused. Disabled = Disable clock.
ClkReq for Clock8	Platform-POR / Enabled / Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock9 assignment	Platform-POR / Enabled / Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabledeven if unused. Disabled = Disable clock.

Menu Item	Options	Description
ClkReq for Clock9	Platform-POR / Enabled / Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.

SATA Configuration

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-IO Configuration ⇨ SATA Configuration

Menu Item	Options	Description
SATA Controller(s)	Enabled / Disabled	Enable or disable SATA Device.
SATA Mode Selection	AHCI	Determine how SATA controller(s) operate.
SATA Test Mode	Enabled / Disabled	Test Mode enable/disable (Loop Back).
SATA Speed	Gen 1 / Gen 2 / Gen 3	SATA Speed
Software Feature Mask Configuration	See submenu	RST Legacy OROM/RST UEFI driver will refer to the SWFM configuration to enable/disable the storage features.
Aggressive LPM Support	Enabled / Disabled	Enable PCH to aggressively enter link power state.
Port X	Enabled / Disabled	Enable or Disable SATA Port
Hot Plug	Enabled / Disabled	Designates this port as Hot Pluggable.
External	Enabled / Disabled	Marks this port as external.
Spin Up Device	Enabled / Disabled	If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive / Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.
Topology	Unknown / ISATA / Direct Connect / Flex / M2	Identify the SATA topology if it is Default or ISATA or Flex or DirectConnect or M2.
SATA Port X DevSlp	Enabled / Disabled	Enable/Disable SATA Port 0 DevSlp. For DevSlp to work, both hard drive and SATA port need to support DevSlp function, otherwise an unexpected behaviour might happen. Please check board design before enabling it.
DITO Configuration	Enabled / Disabled	Enable or Disable DITO configuration.

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-IO Configuration ⇨ SATA Configuration ⇨ Software Feature Mask Configuration

Menu Item	Options	Description
Software Feature Mask Configuration		

USB Configuration

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

Menu Item	Options	Description
xDCI Support	Enabled / Disabled	Enable/Disable xDCI (USB OTG Device)
USB2 PHY Sus Well Power Gating	Enabled / Disabled	Select “Enabled” to enable SUS Well PG for USB2 PHY. This option has no effect on PCH-H
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

Menu Item	Options	Description
		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 consumption.
USB3.1 Portx Speed Selection	[X]	Port Selection value in decimal for Gen1, Default –Gen2; Bit 0 corresponds to Port 0 and so on.
USB Port Disable Override	Enabled / Disabled	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.

Security Configuration

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ 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.

HDA Audio Configuration

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ 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.

Seriallo Configuration

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

Menu Item	Options	Description
I2C0 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller if given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1, 2, 3 UART0 and UART1, SPIO, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 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)
I2C4 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller For I2C5 and UART2 to work this device has to be enabled
I2C5 Controller	Enabled / Disabled / Post Code Only	Enables/Disables Seriallo Controller For this device to work I2C4 has to be enabled
I2C6 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller if given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1, 2, 3 UART0 and UART1, SPIO, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot

Menu Item	Options	Description
		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)
I2C7 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller if given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1, 2, 3 UART0 and UART1, SPIO, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 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)
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 CFG Space will still be visible. This is needed functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1, 2, 3 UART0 and UART1, SPIO, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 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 CFG Space will still be visible. This is needed functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1, 2, 3 UART0 and UART1, SPIO, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 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	Enabled / Disabled	Enables/Disables Seriallo SPI2 Controller. The following device depends from: Thermal Subsystem in PC1 mode Otherwise SPI2 will not appear in the OS
SPI3 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller if given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1, 2, 3 UART0 and UART1, SPIO, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 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)
SPI4 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller if given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1, 2, 3 UART0 and UART1, SPIO, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 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)
SPI5 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller if given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1, 2, 3 UART0 and UART1, SPIO, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 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)
SPI6 Controller	Enabled / Disabled	Enables/Disables Seriallo Controller if given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1, 2, 3 UART0 and UART1, SPIO, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 1. Child device is enabled like CNVi Bluetooth

Menu Item	Options	Description
		(_SB.PC00. UA00. BTH0) UART 0 (00:30:00) cannot be enabled when: 1. I2S Audio codec is enabled (_SB.PC00. I2C0. HDAC)
UART0 Controller	Enabled / 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 / Communication port (COM)	Enables/Disables Seriallo Controller if given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1, 2, 3 UART0 and UART1, SPIO, 1 UART2 and I2C4, 5 UART 0 (00:30:00) cannot be disabled when: 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)
Serial IO UART0 Settings	See submenu	Configure Seriallo Controller
Serial IO UART1 Settings	See submenu	Configure Seriallo Controller

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-IO Configuration ⇨ Seriallo Configuration ⇨ Serial IO UART0 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
Power Gating	Enabled / Disabled / Auto	Disabled: No _PS0 _PS3 support, device is left in D0, after initialization. Enabled: _PS0 and _PS3 detection through ACPI if device was initialized prior to first PG. If it was used (DBG2) PG is disabled

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-IO Configuration ⇨ Seriallo Configuration ⇨ Serial IO UART01 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
Power Gating	Enabled / Disabled / Auto	Disabled: No _PS0 _PS3 support, device is left in D0, after initialization. Enabled: _PS0 and _PS3 detection through ACPI if device was initialized prior to first PG. If it was used (DBG2) PG is disabled

SCS Configuration

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-IO Configuration ⇨ SCS Configuration

Menu Item	Options	Description
eMMC 5.1 Controller	Enabled / Disabled	Enable or Disable SCS eMMC 5.1 Controller
UFS 2.0 Controller 1	Enabled / Disabled	Enable or Disable UFS 2.0 Controller

6.6.2.2.7 PCH-FW Configuration

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-FW Configuration

Menu Item	Option	Description
Firmware Update Configuration	See submenu	Configure Management Engine Technology parameters.
PTT Configuration	See submenu	Configure PTT
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 ⇨ RC Advanced Menu ⇨ 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.
FW Update	Enabled / Disabled	Enable/Disable ME FW Update function.

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ PCH-FW Configuration ⇨ PTT Configuration

Menu Item	Option	Description
PTT Capability / State	N/A	Platform Trust Technology Capability / Enablement State

6.6.2.2.8 ACPI D3Cold settings

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ 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

6.6.2.3 Boot Configuration

Setup Utility ⇨ Advanced ⇨ Boot Configuration

Menu Item	Option	Description
Numlock	[X]	Selects Power-on state for Numlock

6.6.2.4 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

6.6.2.5 Chipset Configuration

Setup Utility ⇨ Advanced ⇨ Chipset Configuration

Menu Item	Option	Description
Platform Trust Technology	Enabled / Disabled	Enable/Disable Platform Trust Technology

6.6.2.6 ACPI Table/Features Control

Setup Utility ⇨ Advanced ⇨ ACPI Table/Feature Control

Menu Item	Option	Description
FACP - RTC S4 Wakeup	Enabled / Disabled	Value only for ACPI. Enable/Disable for S4 Wakeup from RTC
APCI – IO APIC Mode	Enabled / Disabled	This is item 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
FACP – Fixed Power Button	Enabled / Disabled	Enable/Disable the FACP Fixed Power Button feature. If SOIx is enabled, the fixed power button will be disabled.
DSDT – APIC Power Button	Enabled / Disabled / Auto	Controls the APIC power button, please disable this option if fixed power button is enabled for FWTS.
RC ACPI Settings	See submenu	

Setup Utility ⇨ Advanced ⇨ ACPI Table/Feature Control ⇨ RC 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
ACPI S3 Support	Enabled / Disabled	Enable ACPI S3 support
Native PCIE Enable	Enabled / Disabled	Bit – PCIe Native * control 0 – ~ Hot Plug 1 – SHPC Native Hot Plug control 2 – ~ Power Management Events 3 – PCIe Advanced Error Reporting control 4 – PCIe Capability Structure control 5 – Latency Tolerance Reporting control
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
D3 Setting for Storage	Disabled / D3Hot	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 enabled, it also disable 8254 timer for SLP_S0 support.
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

6.6.2.7 SIO TQMx86

Setup Utility ⇨ Advanced ⇨ SIO TQMx86

Menu Item	Option	Description
Serial Port X	Enabled / Disabled / Auto	Disabled: No configuration Enabled: User Configuration Auto: EFI/OS chooses configuration
Base I/O Address	2E8 / 2F8 / 3E8 / 3F8	Configure Base I/O Address of corresponding Serial Port X.
Interrupt	IRQ3 / IRQ4 / IRQ5 / IRQ6 / IRQ7	Configure Interrupt of corresponding Serial Port X.
Handshake RTS/CTS	Connected / Disconnected	Connect or disconnect the COM Express Serial Port Handshake RTS/CTS for Serial Port X.
GPI Interrupt Configuration	Interrupt disabled / IRQ7 / IRQ9 / IRQ12	Configure the GPI interrupt number. Note: The interrupt is level high-triggered (ISA-stayle).
Enable USB Overcurrent pins	Enabled / Disabled	Enable the USB Overcurrent signal pins. Note: Hw design have to be prepared to use USB OC pins, like it is described in SMARC specification 2.1

6.6.2.8 Console Redirection Configuration

Setup Utility ⇨ Advanced ⇨ Console Redirection Configuration

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
Terminal Type	VT_100 / VT_100+ / VT_UTF8 / PC_ANSI	Select the Console Redirection terminal type.
Baud Rate	115200 / 57600 / 38400 / 19200 / 9600 / 4800 / 2400 / 1200	Select the Console Redirection Baud Rate.
Data Bits	7 Bits / 8 Bits	Select the Console Redirection Data Bits.
Parity	None / Even / Odd	Select the Console Redirection Parity Bits.
Stop Bits	1 Bit / 2 Bits	Select the Console Redirection Stop Bits.
Flow Control	None / RTS/CTS / XON/XOFF	Select the Console Redirection Flow Control type.
Information Wait Time	0 Second / 2 Second / 5 Second / 10 Second / 30 Second	Select the Console Redirection Port information display time.
C.R. After Legacy Boot	Yes / No	Console Redirection continue works after Legacy Boot.
Text Mode Resolution	AUTO / Force 80×25 / Force 80×24 (DEL FIRST ROW) / Force 80×24 (DEL LAST ROW)	Console Redirection Text Mode Resolution. Auto: Follow VGA text mode Force 80×25: Don't care about VGA and force text mode to be 80×25 Force 80×24 (DEL FIRST ROW): Don't care about VGA and force text mode to be 80×24 and Del first row Force 80×24 (DEL LAST ROW): Don't care about VGA and force text mode to be 80×24 and Del last row
Auto Refresh	Enabled / Disabled	When feature enable, screen will be auto refresh once after detect remote terminal was connected.

Menu Item	Options	Description
Auto adjust Terminal resolution	Enabled / Disabled	Through send extra ESC sequence code
COM_X	See submenu	Set parameters of COM Express Serial Port X. Whereby X stands for COM Express Serial Port 0 (Insyde name COMA) or 1 (Insyde name COMB).

Note: All COM / HSUART submenu are identical and thus will be listed only once.

Menu Item	Options	Description
PortEnable	Enabled / Disabled	Enable or disable corresponding port.
UseGlobalSetting	Enabled / Disabled	If enabled use settings defined in superordinate CR menu. Disabling this option unhides corresponding settings.

6.6.2.9 H20Uve Configuration

Setup Utility ⇨ Advanced ⇨ H20Uve Configuration

Menu Item	Option	Description
H20Uve	Enabled / Disabled	Enable or disable interface of settings of SCU for H20Uve tool.

6.6.2.10 H20 Event Log Config Manager

Setup Utility ⇨ Advanced ⇨ H20 Event Log Config Manager

Menu Item	Option	Description
Configuration Pages	See submenu	Show all of the configuration pages.
Event And Message Pages	See submenu	Show all of the Event And Message pages.

Setup Utility ⇨ Advanced ⇨ H20 Event Log Config Manager ⇨ Configuration Pages

Menu Item	Option	Description
BIOS Event Log Configuration	See submenu	Show BIOS Event Log Configuration
POST Message Configuration	See submenu	Shot POST Message Configuration

Setup Utility ⇨ Advanced ⇨ H20 Event Log Config Manager ⇨ Configuration Pages ⇨ BIOS Event Log Configuration

Menu Item	Option	Description
Log Event To	Memory / Disabled	Setting Events to Log Selected Storage
Event Log Full option	Overwrite / Clear All / Stop Logging	Overwrite: Overwrite the oldest event data wirh newer ones. Clear All: Clear All event data. Stop Logging: Stop logging event data.

Setup Utility ⇨ Advanced ⇨ H20 Event Log Config Manager ⇨ Configuration Pages ⇨ POST Message Configuration

Menu Item	Option	Description
POST Message Configuration	Enabled / Disabled	Enable / Disable the POST message settings.
Progress Code	Enabled / Disabled	Progress Code Messages are Enabled/Disabled in the BIOS.

Menu Item	Option	Description
Error Code	Enabled / Disabled	Error Code Messages are Enabled/Disabled in the BIOS.
Debug Code	Enabled / Disabled	Debug Code Messages are Enabled/Disabled in the BIOS.
Log POST Message	Enabled / Disabled	Enabled – POST Message will be logged to BIOS GPNV, BMC SEL or others event Storage. Disabled – Don`t log any POST Message
Show POST Message	Enabled / Disabled	Enabled – POST Message will show on screen after VGA is active. Disabled – Don`t show any POST Message

Setup Utility ⇨ Advanced ⇨ H20 Event Log Config Manager ⇨ Event and Message Pages

Menu Item	Option	Description
BIOS Event Log Viewer	See submenu	Show BIOS Event Log Viewer

Setup Utility ⇨ Advanced ⇨ H20 Event Log Config Manager ⇨ Event and Message Pages ⇨ BIOS Event Log Viewer

Menu Item	Options	Description
Show BIOS Event Log	See submenu	Select the Event Storage to show the events of it.
Clear Event Log	Memory	Select the Event Storage to clear the events of it.

Setup Utility ⇨ Advanced ⇨ H20 Event Log Config Manager ⇨ Event and Message Pages ⇨ BIOS Event Log Viewer ⇨ Show BIOS Event Log

Menu Item	Options	Description
Show BIOS Event Log	Memory	Select the Event Storage to clear the events of it.

6.6.3 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 0.
TPM Operation	[ ] / [X]	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 BIOS password. The length of password must be greater than one and smaller or equal ten characters.

6.6.4 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

Menu Item	Options	Description
Boot Type	Dual Boot Type (non-POR) / Legacy Boot Type (non-POR) / UEFI Boot Type	Select boot type to Dual type, Legacy type or UEFI type.
Quick Boot	Enabled / Disabled	Allow InsydeH2O to skip certain tests while booting. This will decrease the time needed to boot the system.
Quiet Boot	Enabled / Disabled	Enable or disable booting in Text Mode.
Network Stack	Enabled / Disabled	Network Stack Support: Windows 8 Bitlocker Unlock UEFI IPv4/IPv6 PXE Legacy PXE OPROM
Power up In Standby Support	Enabled / Disabled	Enable or disable the Power Up in Standby Support (PUIS). The PUIS feature 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	Position in Boot Order for Shell, Network and Removables.
ACPI Selection	Acpi3.0/ Acpi4.0 / Acpi5.0 / Acpi6.0 / Acpi6.1 / Acpi6.2 / Acpi6.3	Select booting to Acpi3.0/ Acpi4.0 / Acpi5.0 / Acpi6.0 / Acpi6.1 / Acpi6.2 / Acpi6.3
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/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.

Setup Utility ⇨ Boot ⇨ Boot Device Priority

Menu Item	Option	Description
[Shell] Internal UEFI Shell 2.0	[X]	Press F5/F6 to adjust position and select item to enable/disable boot device.

6.6.6 Exit

Menu Item	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
Load Custom Defaults	Load Custom Defaults
Save Custom Defaults	Save Custom Defaults
Discard Changes	Discard Changes

7. BIOS – UPDATE

The uEFI BIOS update instruction serves to guarantee a proper way to update the uEFI BIOS on the TQMxE41S.
Please read the entire instructions before beginning the BIOS update.
By disregarding the information you can destroy the uEFI BIOS on the TQMxE41S!
This document will guide the customer to update the uEFI BIOS on the TQMxE41S by using the Insyde Flash Firmware Tools.
The InsydeH2O Tools are only available on request.
Please contact support@tq-group.com for more information about the BIOS Tools and the latest uEFI BIOS version for the TQMxE41S.

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.

7.1.1 Step 1: Preparing USB Stick

A USB stick with FAT32 format can be used. Copy the following files to the USB stick.
(See: https://www.tq-group.com/de/support/downloads/tq-embedded/software-treiber/x86-architektur/)

- H2OFFT-Sx64.efi (Flash Firmware Tool from Insyde for update via UEFI Shell)
  - Be sure to have H2OFFT Version 200.02.00.10 or later
- InsydeH2OFF_x86_WINx64 folder (Flash Firmware Tool from Insyde for update via Windows 64-bit system)
- BIOS.bin file e.g. xx.bin

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

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

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ 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.

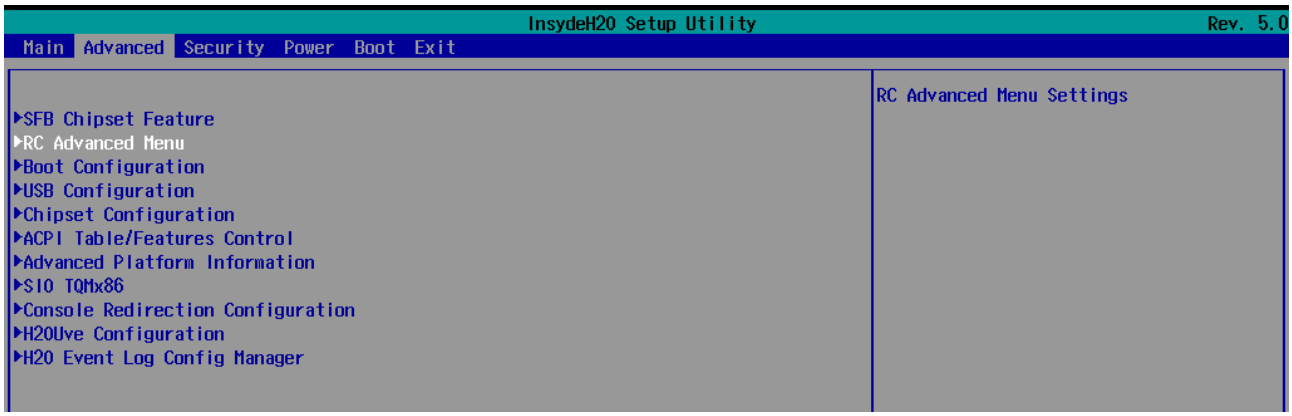

Figure 3: RC Advanced menu

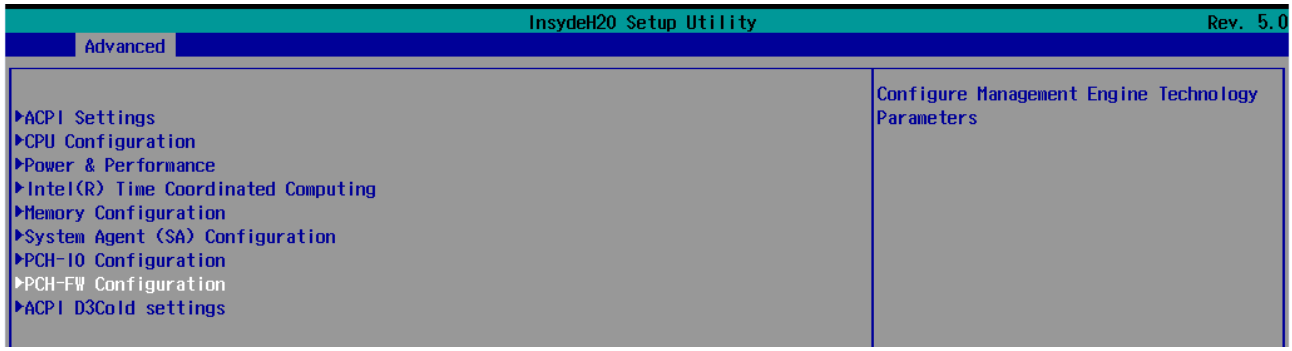

Figure 4: PCH-FW Configuration menu

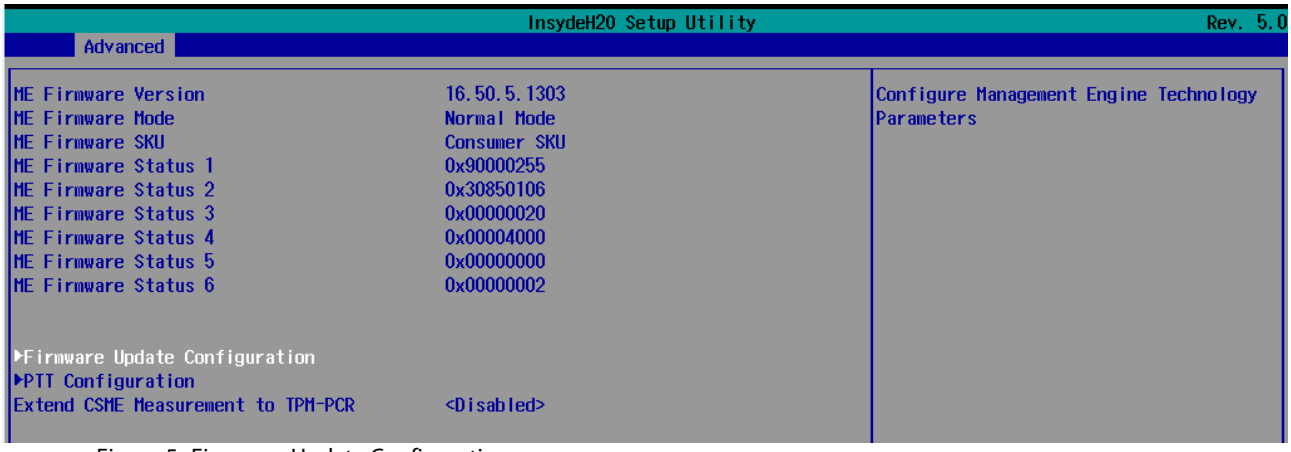

Figure 5: Firmware Update Configuration menu

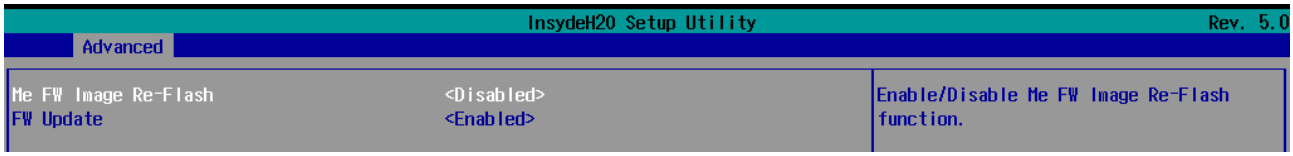

Figure 6: ME FW Image Re-Flash option

7.1.3 Step 3a: Updating uEFI BIOS via EFI Shell

Insert the USB stick into the board on which you want to update the uEFI BIOS and switch on the board. The board will boot and go to the internal EFI shell. Note: If a boot device is plugged change to “Boot Manager” over Front Page and select “Internal EFI Shell”.

Figure 7: 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, enter into the BIOS folder (e.g. “`cd TQMxE41S`”) to execute the Insyde BIOS update tool:

```
H2OFFT-Sx64.efi <BIOS file> -ALL -RA
```

If the argument “-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.

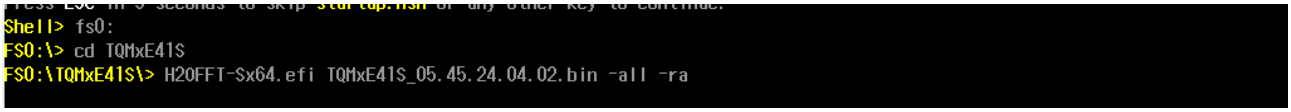

Figure 8: EFI Shell uEFI BIOS Update

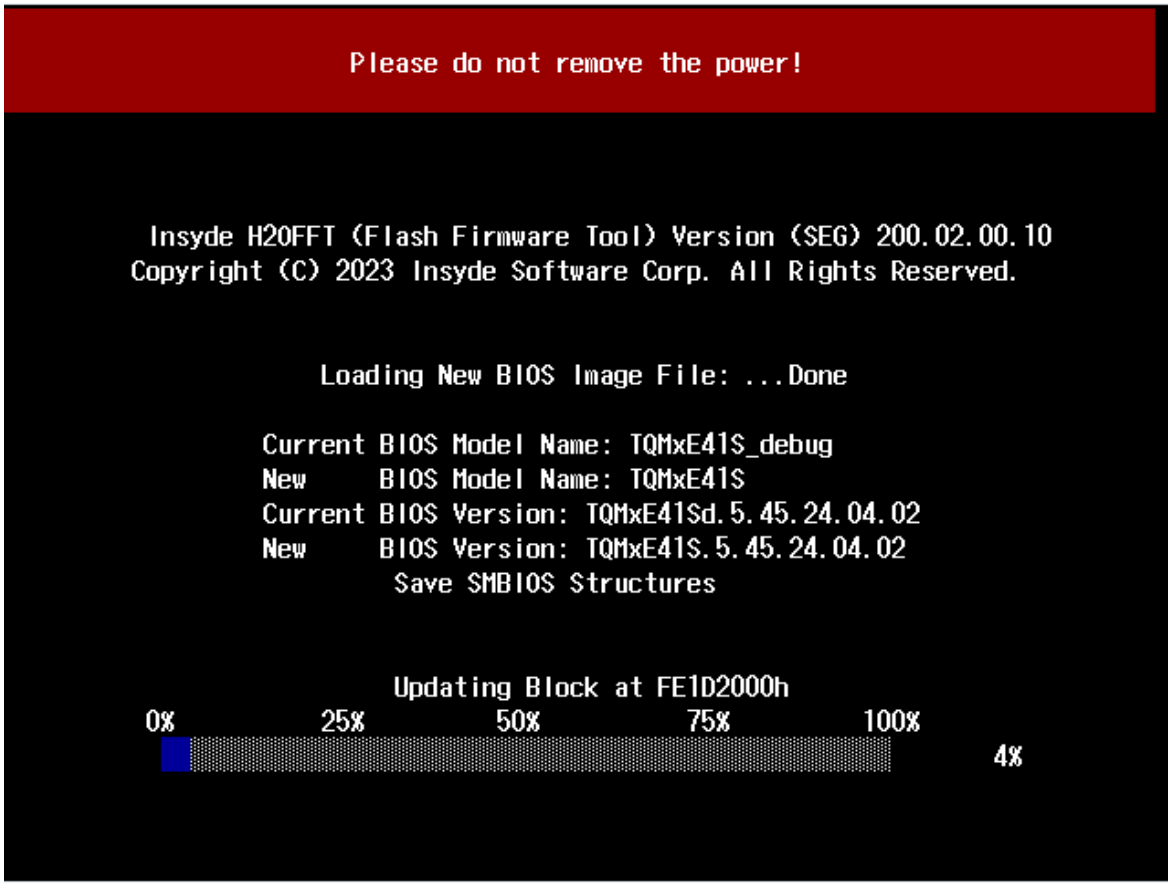

Figure 9: Screen during BIOS Update

7.1.4 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 argument "-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.

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

7.1.5 Step 4: BIOS update check on the TQMxE41S Module

After the uEFI BIOS update, the new uEFI BIOS configures the complete TQMxE41S hardware and this results in some reboots and the first boot time takes longer (up to 1 minute).

The TQMxE41S includes a dual colour Debug LED providing boot and uEFI BIOS information.

If the green LED is blinking the uEFI BIOS is booting. If the green LED is lit permanently the uEFI BIOS boot is finished.

After the uEFI BIOS has been flashed completely, please check whether the uEFI BIOS has been flashed successfully. The BIOS Main menu includes the board and hardware information and it shows the installed BIOS version.

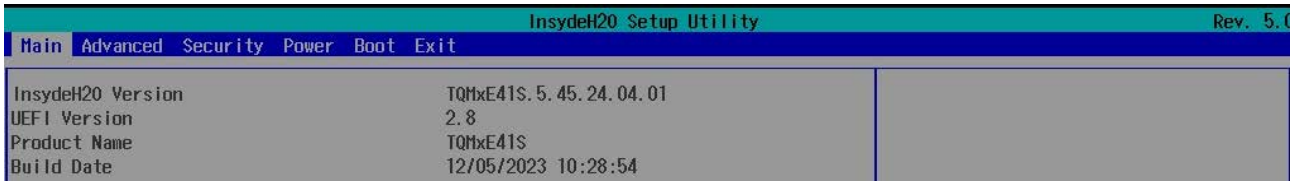

Figure 10: EFI BIOS Main Menu

8. SAFETY REQUIREMENTS AND PROTECTIVE REGULATIONS

8.1 EMC

The TQMxE41S was developed according to the requirements of electromagnetic compatibility (EMC). Depending on the target system, anti-interference measures may still be necessary to guarantee the adherence to the limits for the overall system.

8.2 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 arranged directly at the inputs of a system. As these measures always have to be implemented on the carrier board, no special preventive measures were done on the TQMxE41S.

8.3 Shock & Vibration

The TQMxE41S is designed to be insensitive to shock and vibration and impact.
The design avoids additional connectors like SO-DIMM sockets to support applications also in harsh environments.

8.4 Operational Safety and Personal Security

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

8.5 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.

8.6 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.

8.7 Warranty

TQ-Systems GmbH warrants that the product, when used in accordance with the contract, fulfills 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

8.8 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 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 or 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 reserves the right to update and modify this notice as it deems necessary or appropriate.

8.9 Reliability and Service Life

The MTBF according to MIL-HDBK-217F N2 is 474 544 hours, Ground Benign, at +40 °C.

9. ENVIRONMENT PROTECTION

9.1 RoHS

The TQMxE41S is manufactured RoHS compliant.

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

9.2 WEEE®

WEEE® regulations do not apply since the TQMxE41S cannot operate on its own.

9.3 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.

9.4 EuP

The Ecodesign Directive, also Energy using Products (EuP), is applicable to products for the end user with an annual quantity >200,000. The TQMxE41S must therefore always be seen in conjunction with the complete device.

The available standby and sleep modes of the components on the TQMxE41S enable compliance with EuP requirements for the TQMxE41S.

9.5 Battery

No batteries are assembled on the TQMxE41S.

9.6 Packaging

By environmentally friendly processes, production equipment and products, we contribute to the protection of our environment. To be able to reuse the TQMxE41S, 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 TQMxE41S is delivered in reusable packaging.

9.7 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.

Due to the fact that at the moment there is still 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.

10. APPENDIX

10.1 Acronyms and Definitions

The following acronyms and abbreviations are used in this document:

Table 11: Acronyms

Acronym	Meaning
AHCI	Advanced Host Controller Interface
ATA	Advanced Technology Attachment
BIOS	Basic Input/Output System
BOM	Bill Of Material
CAN	Controller Area Network
CPU	Central Processing Unit
CSM	Compatibility Support Module
DDI	Digital Display Interface
DDR3L	Double Data Rate 3 Low Voltage
DMA	Direct Memory Access
DP	Display Port
DVI	Digital Visual Interface
EAPI	Embedded Application Programming Interface
eDDI	embedded Digital Display Interface
EDID	Extended Display Identification Data
eDP	embedded Display Port
EEPROM	Electrically Erasable Programmable Read-only Memory
EFI	Extensible Firmware Interface
EMC	Electro-Magnetic Compatibility
eMMC	embedded Multi-Media Card
eSATA	external Serial ATA
ESD	Electro-Static Discharge
FAE	Field Application Engineer
FPGA	Field Programmable Gate-Array
FR-4	Flame Retardant 4
FTPM	Firmware Trusted Platform Module
GbE	Gigabit Ethernet
GFX	Graphics
GPI	General Purpose Input
GPIO	General Purpose Input/Output
GPMI	General Purpose Media Interface
GPO	General Purpose Output
GPT	General Purpose Timer
HD	High Definition
HDMI	High Definition Multimedia Interface
HEVC	High Efficiency Video Coding
HFM	High Frequency Mode
HPD	Hot Plug Detection
I	High Definition Audio
I/O	Input Output
I^2C	Inter-Integrated Circuit
IDE	Integrated Device Electronics
IEEE®	Institute of Electrical and Electronics Engineers
IO	Input Output
IoT	Internet of Things
IP	Ingress Protection
IRQ	Interrupt Request
JEIDA	Japan Electronic Industries Development Association
JPEG	Joint Photographic Experts Group
JTAG®	Joint Test Action Group
LED	Light Emitting Diode
LP	Low Power or Low Profile

10.1 Acronyms and Definitions (continued)

Table 11: Acronyms (continued)

Acronym	Meaning
LPC	Low Pin-Count
LVDS	Low Voltage Differential Signal
MISO	Master In Slave Out
MMC	Multimedia Card
MOSI	Master Out Slave In
mPCIe	Mini PCIe
MPEG	Moving Picture Experts Group
mSATA	Mini SATA
MTBF	Mean operating Time Between Failures
N/A	Not Applicable
OD	Open Drain
OpROM	Option ROM
OS	Operating System
PC	Personal Computer
PCB	Printed Circuit Board
PCIe	PCI Express
PCMCIA	People Can't Memorize Computer Industry Acronyms
PD	Pull-Down
PICMG®	PCI Industrial Computer Manufacturers Group
PU	Pull-Up
PWM	Pulse-Width Modulation
RAM	Random Access Memory
RMA	Return Merchandise Authorization
RoHS	Restriction of (the use of certain) Hazardous Substances
ROM	Read-Only Memory
RSVD	Reserved
RTC	Real-Time Clock
SATA	Serial ATA
SCU	System Configuration Utility
SD card	Secure Digital Card
SD/MMC	Secure Digital Multimedia Card
SDIO	Secure Digital Input Output
SDRAM	Synchronous Dynamic Random Access Memory
SGET	Standardization Group for Embedded Technologies
SIMD	Single Instruction Multiple Data
SMARC	Smart Mobility ARChitecture
SMBus	System Management Bus
SO-DIMM	Small Outline Dual In-Line Memory Module
SPD	Serial Presence Detect
SPI	Serial Peripheral Interface
SSD	Solid-State Drive
TBD	To Be Determined
TDM	Time-Division Multiplexing
TDP	Thermal Design Power
TPM	Trusted Platform Module
TPM_PP	Trusted Platform Module Physical Presence
UART	Universal Asynchronous Receiver and Transmitter
uEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VC1	Video Coding (standard) 1
VESA	Video Electronics Standards Association
VP9	Video Playback 9
WDT	Watchdog Timer
WEEE®	Waste Electrical and Electronic Equipment

10.2 References

Table 12: Further Applicable Documents and Links

No.	Name	Rev., Date	Company
(1)	SMARC (Smart Mobility ARChitecture) Hardware Specification	Version 2.1.1, May 20, 2020	SGET
(2)	SMARC (Smart Mobility ARChitecture) Design Guide	Rev. 2.1.1, April 29, 2021	SGET

TQ-Systems GmbH
Mühlstraße 2 I Gut Delling I 82229 Seefeld
tq-group.com I www.tq-group.com

Technology in Quality