



TABLE OF CONTENTS

1.	ABOUT THIS MANUAL.....	1
1.1	Copyright and Licence Expenses.....	1
1.2	Registered Trademarks.....	1
1.3	Disclaimer.....	1
1.4	Imprint.....	1
1.5	Service and Support.....	1
1.6	Tips on Safety.....	2
1.7	Symbols and Typographic Conventions.....	2
1.8	Handling and ESD Tips.....	2
1.9	Naming of Signals.....	3
1.10	Further Applicable Documents / Presumed Knowledge.....	3
2.	INTRODUCTION.....	4
2.1	Functional Overview.....	4
2.2	SMARC Specification Compliance.....	5
2.3	TQMxE40S Variants.....	5
2.4	Accessories.....	5
3.	FUNCTION.....	6
3.1	TQMxE40S Block Diagram.....	6
3.2	Electrical Characteristics.....	6
3.2.1	Supply Voltage.....	6
3.2.2	Power Consumption.....	7
3.2.2.1	Real Time Clock Power Consumption.....	8
3.3	Environmental conditions.....	8
3.4	System Components.....	9
3.4.1	CPUs.....	9
3.4.2	Graphics.....	9
3.4.3	Memory.....	10
3.4.3.1	LPDDR4 SDRAM.....	10
3.4.3.2	eMMC.....	10
3.4.3.3	SPI Boot Flash.....	10
3.4.3.4	EEPROM.....	10
3.4.4	Real Time Clock.....	10
3.4.5	Trusted Platform Module.....	10
3.4.6	TQ flexible I/O configuration (TQ-flexiCFG).....	11
3.5	Interfaces.....	11
3.5.1	PCI Express.....	11
3.5.2	Gigabit Ethernet.....	11
3.5.3	Serial ATA.....	11
3.5.4	Digital Display Interface.....	11
3.5.5	LVDS Interface.....	12
3.5.6	USB 2.0 Interfaces.....	12
3.5.7	USB 3.0 Interfaces.....	12
3.5.8	SD Card Interface.....	12
3.5.9	General Purpose Input/Output.....	12
3.5.10	Audio Interfaces.....	12
3.5.11	CAN interfaces.....	12
3.5.12	I ² C Bus.....	13
3.5.13	SMBus / Power Management I ² C Bus.....	13
3.5.14	Serial Peripheral Interface.....	13
3.5.15	eSPI.....	13
3.5.16	Serial Ports.....	13
3.5.17	Watchdog Timer.....	13
3.6	Connectors & LEDs.....	13
3.6.1	SMARC Connector.....	13
3.6.2	Debug LED.....	14
3.7	SMARC Connector Pinout.....	14
3.7.1	Signal Assignment Abbreviations.....	14
3.7.2	SMARC Connector Pin Assignment.....	15
4.	MECHANICS.....	21



4.1	TQMxE40S Dimensions.....	21
4.2	Heat Spreader Dimensions.....	22
4.3	Mechanical and Thermal Considerations	23
4.4	Protection against external effects.....	23
4.5	Label placement.....	23
5.	SOFTWARE.....	24
5.1	System Resources.....	24
5.1.1	I ² C Bus	24
5.1.2	SMBus	24
5.1.3	Memory Map.....	24
5.1.4	IRQ Map.....	24
5.2	Operating Systems.....	25
5.2.1	Supported Operating Systems.....	25
5.2.2	Driver Download	25
5.3	TQ-Systems Embedded Application Programming Interface (EAPI).....	25
5.4	Software Tools.....	25
6.	BIOS	26
6.1	Continue Boot Process	26
6.2	Boot Manager	26
6.3	Device Manager	27
6.3.1	Driver Health Manager	27
6.3.2	Network Device List.....	27
6.4	Boot From File	27
6.5	Administer Secure Boot.....	27
6.6	Setup Utility	28
6.6.1	Main	28
6.6.2	Advanced.....	28
6.6.2.1	Boot Configuration	29
6.6.2.2	USB Configuration	29
6.6.2.3	Chipset Configuration.....	29
6.6.2.4	ACPI Table/Features Control.....	29
6.6.2.5	RC Advanced Menu	30
6.6.2.6	SIO TQMx86.....	42
6.6.2.7	Console Redirection	43
6.6.2.8	H2OUVE Configuration.....	44
6.6.2.9	SIO F81214E	44
6.6.2.10	NVM Express Information	44
6.6.3	Security.....	44
6.6.4	Power	44
6.6.4.1	CPU Configuration.....	45
6.6.5	Boot	46
6.6.6	Exit	47
6.7	BIOS Update.....	47
6.7.1	Step 1: Preparing USB Stick.....	47
6.7.2	Step 2: Preparing Management Engine (ME) FW for update.....	48
6.7.3	Step 3a: Updating uEFI BIOS via EFI Shell	49
6.7.4	Step 2b: Updating uEFI BIOS via Windows Operating System.....	50
6.7.5	Step 3: BIOS update check on the TQMxE40S Module	51
7.	SAFETY REQUIREMENTS AND PROTECTIVE REGULATIONS.....	52
7.1	EMC.....	52
7.2	ESD.....	52
7.3	Shock & Vibration.....	52
7.4	Operational Safety and Personal Security	52
7.5	Reliability and Service Life	52
8.	ENVIRONMENT PROTECTION.....	53
8.1	RoHS	53
8.2	WEEE®	53
8.3	REACH®.....	53
8.4	EuP	53
8.5	Battery.....	53
8.6	Packaging	53
8.7	Other Entries.....	53
9.	APPENDIX	54
9.1	Acronyms and Definitions	54
9.2	References	56



TABLE DIRECTORY

Table 1:	Terms and Conventions	2
Table 2:	TQMxE40S Power Consumption	7
Table 3:	RTC Current Consumption	8
Table 4:	Intel® X6000E Series: Comparison of the SKUs.....	9
Table 5:	Maximum Resolution	10
Table 6:	PCI Express Configuration Options.....	11
Table 7:	LED Boot Messages.....	14
Table 8:	Abbreviations used.....	14
Table 9:	SMARC Connector Pin Assignment	15
Table 10:	I ² C Address Mapping on GP I ² C Port.....	24
Table 11:	Acronyms.....	54
Table 12:	Further Applicable Documents and Links	56

FIGURE DIRECTORY

Figure 1:	Block Diagram TQMxE40S	6
Figure 2:	Three-sided drawing TQMxE40S (dimensions in mm)	21
Figure 3:	Bottom view drawing TQMxE40S.....	21
Figure 4:	Standard Heat Spreader TQMxE40S-HSP (dimensions in mm)	22
Figure 5:	InsydeH2O BIOS Front Page.....	26
Figure 6:	RC Advanced Menu	48
Figure 7:	PCH-FW Configuration menu	48
Figure 8:	Firmware Update configuration menu.....	48
Figure 9:	ME FW Image Re-Flash option	49
Figure 10:	EFI Shell	49
Figure 11:	EFI Shell uEFI BIOS Update	49
Figure 12:	Screen during BIOS Update.....	50
Figure 13:	TQMxE40S Debug LED.....	51
Figure 14:	EFI BIOS Main Menu.....	51

REVISION HISTORY

Rev.	Date	Name	Pos.	Modification
0100	29-10-2021	Kreuzer		Initial release
0101	30-06-2022	Kreuzer	Figure 1	Correction: Ethernet 1 PHY is connected to SGMII



1. ABOUT THIS MANUAL

1.1 Copyright and Licence Expenses

Copyright protected © 2022 by TQ-Systems GmbH.

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

	<p>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.</p> <p>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.</p> <p>Violation of this guideline may result in damage / destruction of the TQMxE40S and be dangerous to your health.</p> <p>Improper handling of your TQ-product would render the guarantee invalid.</p>
---	--

Proper ESD handling

	<p>The electronic components of your TQ-product are sensitive to electrostatic discharge (ESD).</p> <p>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.</p>
---	--



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 TQMxE40S is based on the latest generation of Intel® Atom™, Pentium® and Celeron® CPUs (code name “Elkhart Lake”). It achieves a new level of computing performance, security and media processing performance in a very compact form factor to empower real-time computing, industrial automation, digital surveillance, aviation, medical, retail and more.

The TQMxE40S corresponds to the internationally established SGET standard SMARC (V2.1). 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 TQMxE40S 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 TQMxE40S perfectly fits for mobile, low power, low profile and battery driven applications in multiple vertical markets like industrial automation, medical devices, transportation and others.

2.1 Functional Overview

The following key functions are implemented on the TQMxE40S:

CPU:

- Intel® Atom® X6000E Series: „Elkhart Lake“ with different SKUs
- optimized for Embedded, Industrial Functional Safety or PC Client applications

Memory:

- LPDDR4/4x: 4 Gbyte, 8 Gbyte, 16 Gbyte with up to 4267MT/s and optional In Band ECC (IBECC)
- eMMC 5.1 on-board flash
- EEPROM: 32 kbit

Graphics:

- 2 × Digital Display Interface (DDI) (DP 1.2/1.3/1.4, HDMI 1.4b/2.0b)
- 1 × Embedded Digital Display Interface (eDDI) or LVDS interface (eDP 1.3 or LVDS)

Peripheral interfaces:

- 2 × Gigabit Ethernet (Marvell 88E1512)
- 1 × SATA 3.0 (up to 6 Gb/s), eSATA capable
- 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; master/slave capable)
- 1 × SMBus
- 1 × SPI (for external uEFI BIOS flash)
- 1 × eSPI interface
- 4 × Serial port (Rx/Tx, legacy compatible)
- 2 × CAN interface
- 1 × SD card interface
- 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
- Extended Temperature: -40 °C to +85 °C

Form factor / dimensions:

- SMARC short form factor; 82 mm × 50 mm

2.2 SMARC Specification Compliance

The TQMxE40S is compliant to the SMARC Hardware Specification (Version 2.1).

2.3 TQMxE40S Variants

The TQMxE40S is available in several standard configurations:

Please visit www.tq-group.com/TQMxE40S for a complete list of standard variants.

Other configurations are available on request.

Standard configuration features are:

- eDP or LVDS
- CPU version
- Memory configuration (RAM / eMMC)
- TPM
- Temperature range

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

TQMxE40S-HSP: Heat spreader for TQMxE40S 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 × USB 3.0, 1 × USB 2.0, HDA and I²S Audio, Micro SD card, 3 × M.2 socket (Key E, B, M), PCIe socket, up to 6 serial interfaces, 2 × CAN

3. FUNCTION

3.1 TQmxE40S Block Diagram

The following illustration shows the block diagram of the TQmxE40S:

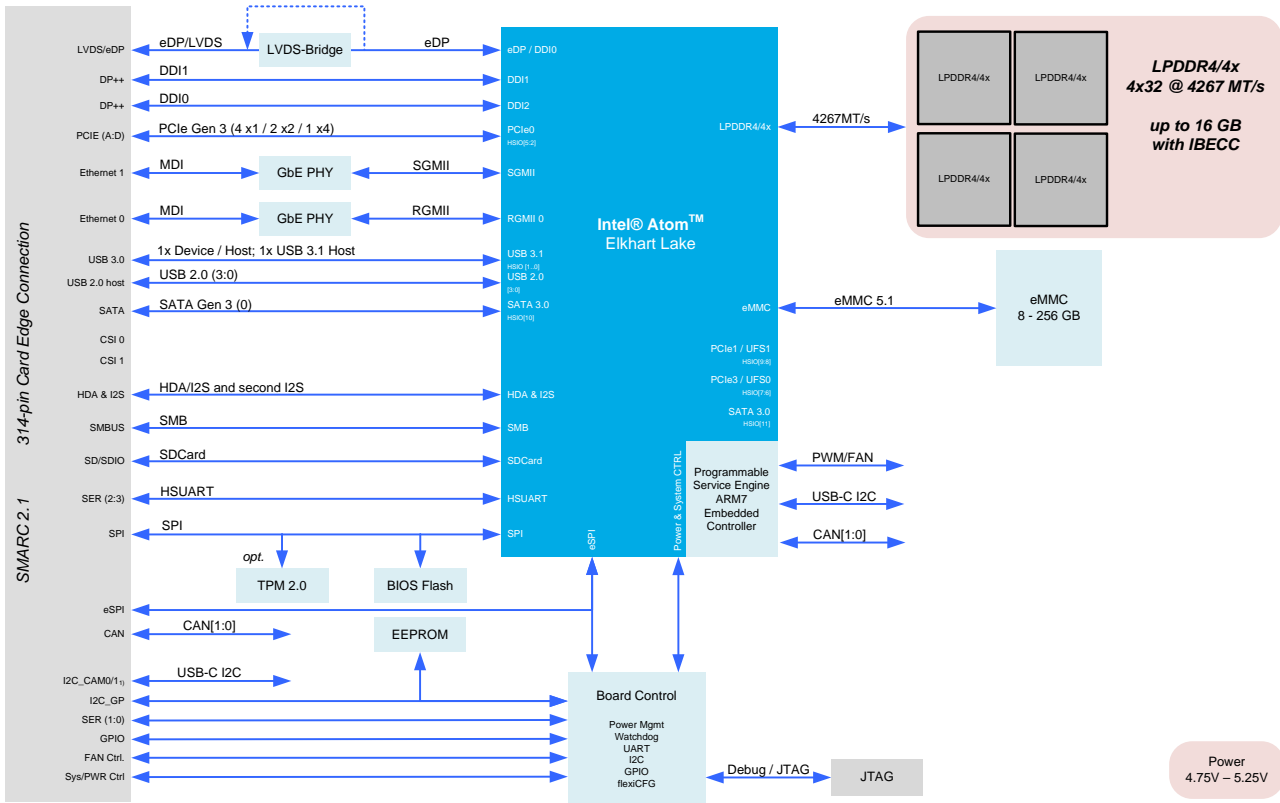


Figure 1: Block Diagram TQmxE40S

3.2 Electrical Characteristics

3.2.1 Supply Voltage

The TQmxE40S 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 TQMxE40S.

The values were measured using the TQMxE40S and the MB-SMARC-3 carrier board.

The measurement was done with two power supplies, one for the TQMxE40S and one for the MB-SMARC-3 carrier board.

The power consumption of each TQMxE40S was measured running Windows® 10, 64 bit and different LPDDR4x configurations. All measurements were done at a temperature of +25 °C and an input voltage of +5.0 V.

The power consumption of the TQMxE40S 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 port is disconnected.
- **Windows 10, 64 bit, idle:**
Desktop idles, Ethernet port is 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, Ethernet port is connected (1000 Mbps Speed)
- **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: TQMxE40S Power Consumption

Module	Mode		
	Suspend (OS shut down)	Win10, 64 bit idle	Win10, 64 bit max. load
SKU6 Atom® x6413E	1.02 W	5.6 W	11.6 W
SKU7 Atom® x6425E	1.02 W	5.8 W	14.8 W
SKU8 Atom® x6212RE	1.02 W	4.8 W	8.4 W
SKU9 Atom® x6414RE	1.02 W	5.4 W	11.5 W
SKU10 Atom® x6425RE	1.02 W	5.8 W	14.6 W

Note: Power requirement



The power supplies on the carrier board for the TQMxE40S must be designed with enough reserve. The carrier board should provide at least twice the maximum workload power of the TQMxE40S. The TQMxE40S 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® X6000E Series “Elkhart Lake”	3.0 V	3 µA

The current consumption of the RTC in the Intel® X6000E Series “Elkhart Lake” in the Product Family Datasheet (EDS) is specified with 6 µA max at room temperature while the system is off. The values measured on several modules were lower than 3µA.

3.3 Environmental conditions

- Operating Temperature Standard: 0 °C to +60 °C
- Operating Temperature Extended: -40 °C to +85 °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 TQMxE40S 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 TQMxE40S supports the Intel® X6000E Series.

The following list shows some key features of these CPUs:

- Quad and dual CPU cores with up to 3GHz
- Intel® 64 Architecture
- Intel® Virtualization Technology (VT)
- In-Band ECC support
- Intel® Streaming SIMD Extensions 4.2 (Intel® SSE4.2)
- Intel® Enhanced Intel® SpeedStep® technology
- Intel® UHD Graphics
- 4 Mbyte Cache
- Triple independent displays

Table 4: Intel® X6000E Series: Comparison of the SKUs

Mode	Atom® x6211E	Atom® x6413E	Atom® x6425E	Atom® x6212RE	Atom® x6414RE	Atom® x6425RE	Atom® x6200FE	Atom® x6427FE
Use Condition	Embedded	Embedded	Embedded	Industrial	Industrial	Industrial	Industrial (FuSA)	Industrial (FuSA)
CPU Cores	2	4	4	2	4	4	2	4
CPU frequency	1.3 GHz	1.5 GHz	2 GHz	1.2 GHz	1.5 GHz	1.9 GHz	1.0 GHz	1.9 GHz
Burst frequency	3 GHz	3 GHz	3 GHz	--	--	--	--	--
UHD Graphics (Execution Units)	16 EUs	16 EUs	32 EUs	16 EUs	16 EUs	32 EUs	None	32 EUs
Temperature T _{junction}	-40 °C to +105 °C	-40 °C to +105 °C	-40 °C to +105 °C	-40 °C to +110 °C	-40 °C to +110 °C	-40 °C to +110 °C	-40 °C to +110 °C	-40 °C to +110 °C
Memory Speed	3200 MT/s	3200 MT/s	3733 MT/s	3200 MT/s	3200 MT/s	4267 MT/s	2400 MT/s	4267 MT/s
Functional Safety	No	No	No	No	No	No	Yes	Yes
Thermal Design Power (TDP)	6 W	9 W	12 W	6 W	9 W	12 W	4.5 W	12 W

3.4.2 Graphics

The Intel® X6000E Series CPUs includes an integrated Intel® UHD (Gen 11) graphics accelerator. It provides excellent 2D/3D graphics performance with dual simultaneous display support.

The following list shows some key features of the Intel® X6000E Series CPUs:

- Graphics Technology (Gen 11 LP) with up to 32 Execution Units
- Hardware accelerated video decoding/encoding for H.264, MPEG2, MVC, VC-1, WMV9, H.265/HEVC, VP9, JPEG/MJPEG
- DirectX 12 support
- OpenGL 4.5, OpenCL 1.2 support

The TQMxE40S supports two Digital Display Interface (DDI) 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	4096 × 2160 at 60 Hz
DP	4096 × 2160 at 60 Hz
HDMI 2.0b	4096 × 2160 at 60 Hz


3.4.3 Memory

3.4.3.1 LPDDR4 SDRAM

The TQMxE40S supports a memory-down 4x32bit LPDDR4x configuration running at up to 4267 MT/s and optional In Band ECC (IB ECC). 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 TQMxE40S supports up to 256 Gbyte on-board eMMC 5.1 flash. The eMMC interface is not activated in BIOS default settings.

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

3.4.3.3 SPI Boot Flash

The TQMxE40S provides a 256 Mbit SPI boot flash. It includes the uEFI BIOS and the Intel® Converged Security Engine (CSE) which is comparable to Trusted Execution Engine (TXE).

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

3.4.3.4 EEPROM

On the TQMxE40S 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 TQMxE40S includes a standard RTC (Motorola MC146818B) integrated in the Intel® X6000E Series CPU.

3.4.5 Trusted Platform Module

The TQMxE40S supports the Trusted Platform Module (TPM) 2.0 (Infineon SLB9670 controller).

Intel® X6000E 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 TQMxE40S 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 TQMxE40S with Intel® X6000E 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

COM Express™ Port 0 – 3				Configuration	Configuration
0	1	2	3	4 ports x1 Lane	Configuration in the BIOS
0		2	3	1 Port X2 Lanes + 2 Ports X1 Lane	Configuration via custom BIOS
0		2		1 Port X2 Lanes + 1 Port X2 Lanes	Configuration via custom BIOS
0				1 Port X4 Lanes	Configuration via custom BIOS

3.5.2 Gigabit Ethernet

The TQMxE40S provides two Marvell 88E1512 Ethernet PHY with 10/100/1000 Mbps speed.

The Ethernet LED functionality defined in the SMARC specification is currently not supported by the TQMxE40S module. Intel is working on this issue.

3.5.3 Serial ATA

The TQMxE40S supports one SATA Gen3.0 interface which supports up to 6 Gb/s.

The integrated SATA host controller supports AHCI mode, the SATA controller no longer supports legacy IDE mode using I/O space.

3.5.4 Digital Display Interface

The TQMxE40S supports three Digital Display Interfaces (DDIO, DDI1 & DDI2) 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 (DP++) or HDMI/DVI with an appropriate level shifter or retimer on the carrier board. Due to signal integrity and flexibility reasons there is no HDMI level shifter realized on the module.

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

The TQMxE40S supports the following maximum display resolutions:

- DisplayPort 1.4 up to 4096 × 2160 at 60 Hz
- Embedded DisplayPort 1.3 up to 4096 × 2160 at 60 Hz
- HDMI 2.0b up to 4096 × 2160 at 60 Hz
- HDMI 1.4b up to 3840 × 2160 @ 30 Hz

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

3.5.5 LVDS Interface

The TQMxE40S 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 TQMxE40S 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, SuperSpeed signals must be taken into account when designing a carrier.

3.5.7 USB 3.0 Interfaces

The TQMxE40S 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 SD Card Interface

The TQMxE40S provides an SD card interface for 4-bit SD/MMC cards at the SMARC connector.

3.5.9 General Purpose Input/Output

The TQMxE40S 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.

3.5.10 Audio Interfaces

The TQMxE40S 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 TQMxE40S. 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.

3.5.11 CAN interfaces

The TQMxE40S provides two CAN interfaces. If a CAN interface is required, corresponding transceivers must be implemented on the carrier.



3.5.12 I²C Bus

The TQMxE40S 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.

3.5.13 SMBus / Power Management I²C Bus

The TQMxE40S provides an I²C based System Management Bus (SMBus) interface. This bus is also called Power Management I²C Bus.

3.5.14 Serial Peripheral Interface

The TQMxE40S provides an SPI interface. The SPI interface can only be used for SPI boot Flash devices.

3.5.15 eSPI

The TQMxE40S provides an eSPI interface where appropriate UARTs or SuperI/Os can be connected.

3.5.16 Serial Ports

The TQMxE40S 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 HSUART (High Speed UART) of the Intel® X6000E Series CPU.

TQ recommends preferring the usage of SER0 and SER1. There might be software compatibility or driver problems when using the Intel® SIO UARTs.

3.5.17 Watchdog Timer

The TQMxE40S 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 TQMxE40S 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 TQMxE40S 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 TQMxE40S SMARC connector pin assignment, which is compliant with the SMARC hardware specification Version 2.1.

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 TQMxE40S.



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	N/A
P4	CSI1_CK-	CSI differential clock input	I	LVDS D-PHY	N/A
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	N/A
P8	CSI1_RX0-	CSI differential data input	I	LVDS D-PHY	N/A
P9	GND	Ground	GND		
P10	CSI1_RX1+	CSI differential data input	I	LVDS D-PHY	N/A
P11	CSI1_RX1-	CSI differential data input	I	LVDS D-PHY	N/A
P12	GND	Ground	GND		
P13	CSI1_RX2+	CSI differential data input	I	LVDS D-PHY	N/A
P14	CSI1_RX2-	CSI differential data input	I	LVDS D-PHY	N/A
P15	GND	Ground	GND		
P16	CSI1_RX3+	CSI differential data input	I	LVDS D-PHY	N/A
P17	CSI1_RX3-	CSI differential data input	I	LVDS D-PHY	N/A
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	
P22	GBE0_LINK1000#	Link Speed Indication LED for 1000 Mbps	OD	3.3 V tolerant	
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	
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	
P34	SDIO_CMD	SD Card: Command line	IO	3.3 V	
P35	SDIO_CD#	SD Card: Card Detect	I PU	3.3 V	
P36	SDIO_CK	SD Card: Clock	O	3.3 V	
P37	SDIO_PWR_EN	SD Card: Power enable	O	3.3 V	
P38	GND	Ground	GND		
P39	SDIO_D0	SD Card: data path	IO	3.3 V	
P40	SDIO_D1	SD Card: data path	IO	3.3 V	
P41	SDIO_D2	SD Card: data path	IO	3.3 V	
P42	SDIO_D3	SD Card: data path	IO	3.3 V	
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 master chip select	O	1.8 V	
P55	ESPI_CS1#	ESPI master chip select	O	1.8 V	
P56	ESPI_CK	ESPI master clock output	O	1.8 V	
P57	ESPI_IO_1	ESPI master data I/O	IO	1.8 V	
P58	ESPI_IO_0	ESPI master data I/O	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 (can be pulled low by TQMxE40S)	IO PU	3.3 V	
P78	PCIE_A_CKREQ#	PCIe Port A clock request (can be pulled low by TQMxE40S)	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++	DP++ only
P93	HDMI_D2- / DP1_LANE0-	TMDS / HDMI data differential pair / DP data pair	O	DP++	DP++ only
P94	GND	Ground	GND		
P95	HDMI_D1+ / DP1_LANE1+	TMDS / HDMI data differential pair / DP data pair	O	DP++	DP++ only
P96	HDMI_D1- / DP1_LANE1-	TMDS / HDMI data differential pair / DP data pair	O	DP++	DP++ only
P97	GND	Ground	GND		
P98	HDMI_D0+ / DP1_LANE2+	TMDS / HDMI data differential pair / DP data pair	O	DP++	DP++ only
P99	HDMI_D0- / DP1_LANE2-	TMDS / HDMI data differential pair / DP data pair	O	DP++	DP++ only
P100	GND	Ground	GND		
P101	HDMI_CK+ / DP1_LANE3+	HDMI differential clock output pair / DP data pair	O	DP++	DP++ only
P102	HDMI_CK- / DP1_LANE3-	HDMI differential clock output pair / DP data pair	O	DP++	DP++ only
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 I ² C clock / DP AUX Channel	IO	DP++ /3.3 V	PU at high AUX_SEL
P106	HDMI_CTRL_DAT / DP1_AUX-	HDMI I ² C data / DP AUX Channel	IO	DP++ /3.3 V	PU at high AUX_SEL
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 I ² C bus: SMBus	IO PU	1.8 V	
P122	I2C_PM_DAT	Power management I ² C 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	
P144	CAN0_RX	CAN Receive input	I	1.8 V	
P145	CAN1_TX	CAN Transmit output	O	1.8 V	
P146	CAN1_RX	CAN Receive input	I	1.8 V	
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	



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 configurations differential data / Camera I ² C	O/IO PU	TDMS / 1.8 V	N/A
S2	CSI1_TX- / I2C_CAM1_DAT	Camera configurations differential data / Camera I ² C	O/IO PU	TDMS / 1.8 V	N/A
S3	GND	Ground	GND		
S4	RSVD	Reserved			
S5	CSI0_TX+ / I2C_CAM0_CK	Camera configurations differential data / Camera I ² C	O/IO PU	TDMS / 1.8 V	N/A
S6	CAM_MCK	Master clock output for CSI camera support	O	1.8 V	N/A
S7	CSI0_TX- / I2C_CAM0_DAT	Camera configurations differential data / Camera I ² C	O/IO PU	TDMS / 1.8 V	N/A
S8	CSI0_CK+	CSI differential clock input	I	LVDS D-PHY	N/A
S9	CSI0_CK-	CSI differential clock input	I	LVDS D-PHY	N/A
S10	GND	Ground	GND		
S11	CSI0_RX0+	CSI differential data input	I	LVDS D-PHY	N/A
S12	CSI0_RX0-	CSI differential data input	I	LVDS D-PHY	N/A
S13	GND	Ground	GND		
S14	CSI0_RX1+	CSI differential data input	I	LVDS D-PHY	N/A
S15	CSI0_RX1-	CSI differential data input	I	LVDS D-PHY	N/A
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	
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	
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	N/A
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	I ² S: Master clock output to Audio codecs	O	1.8 V	
S39	I2S0_LRCK	I ² S: Left& Right audio synchronization clock	IO	1.8 V	
S40	I2S0_SDOUT	I ² S: Digital audio Output	O	1.8 V	
S41	I2S0_SDIN	I ² S: Digital audio Input	I	1.8 V	
S42	I2S0_CK	I ² S: 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	
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 I ² C bus	IO PU	1.8 V	
S49	I2C_GP_DAT	General Purpose I ² C bus	IO PU	1.8 V	
S50	HDA_SYNC / I2S2_LRCK	HDA: sync / I ² S: Left& Right audio synchronization clock	IO	1.8 V	
S51	HDA_SDO / I2S2_SDOUT	HDA: data out / I ² S: Digital audio Output	O	1.8 V	
S52	HDA_SDI / I2S2_SDIN	HDA: data in / I ² S: Digital audio Input	I	1.8 V	



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 / I ² S: Digital audio clock	IO	1.8 V	
S54	SATA_ACT#	Active low SATA activity indicator	OD	3.3 V	
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 I ² C 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 I ² C 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	I ² C bus to read display EDID EEPROMs (for LVDS displays)	IO PU	1.8 V	
S140	I2C_LCD_DAT	I ² C 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_PRSN#	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	1.8 V	
S157	TEST#	Held low by carrier for module vendor specific functions	I PU	1.8 V	
S158	GND	Ground	GND		

4. MECHANICS

4.1 TQMxE40S Dimensions

The dimensions of the TQMxE40S are 82 mm × 50 mm.

The following illustration shows the three-sided drawing of the TQMxE40S.

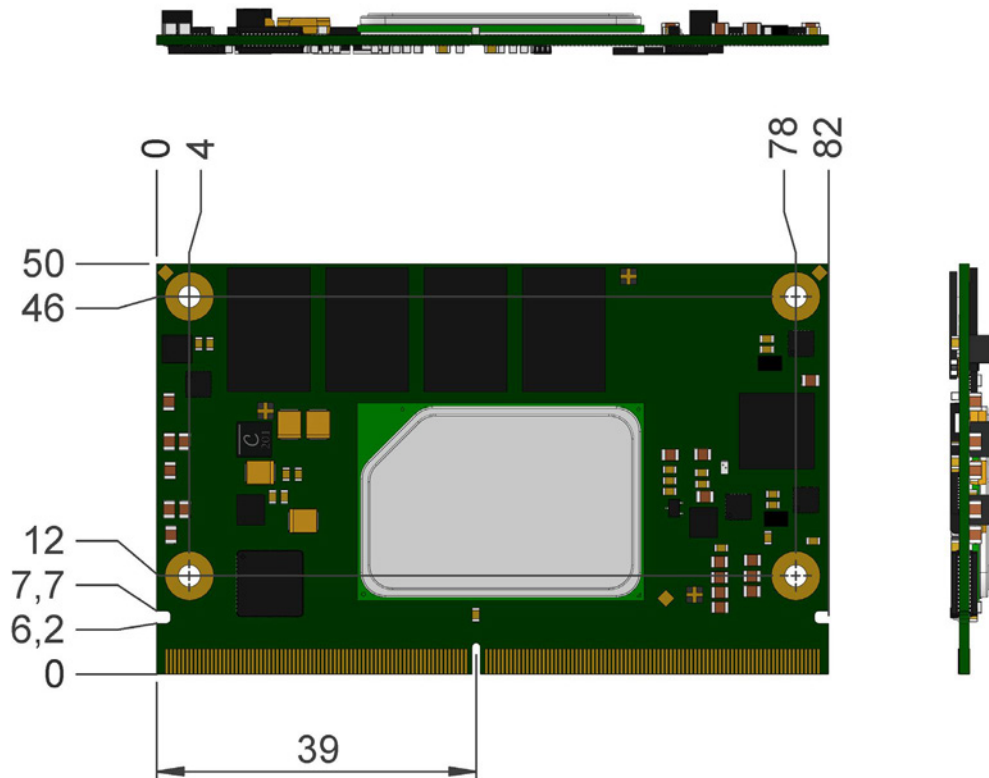


Figure 2: Three-sided drawing TQMxE40S (dimensions in mm)

The following illustration shows the bottom view of the TQMxE40S.

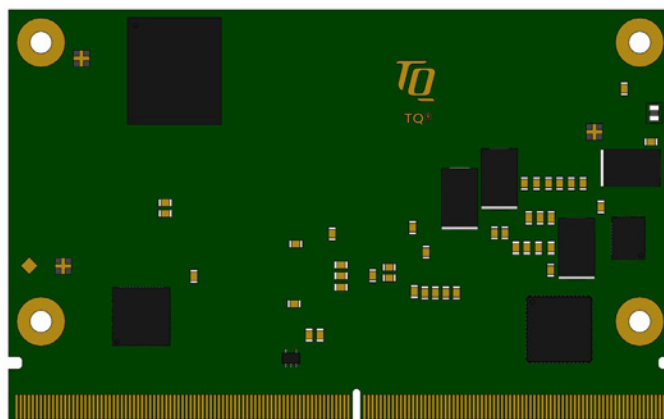


Figure 3: Bottom view drawing TQMxE40S

4.2 Heat Spreader Dimensions

The TQMxE40S supports two different heat spreader versions. Both versions are compliant to the SMARC specification with 6 mm height.

Heat spreader for the Intel® X6000E Series CPU

- **TQMxE40S-HSP**

The following illustration shows the standard heat spreader (TQMxE40S-HSP) for the TQMxE40S.

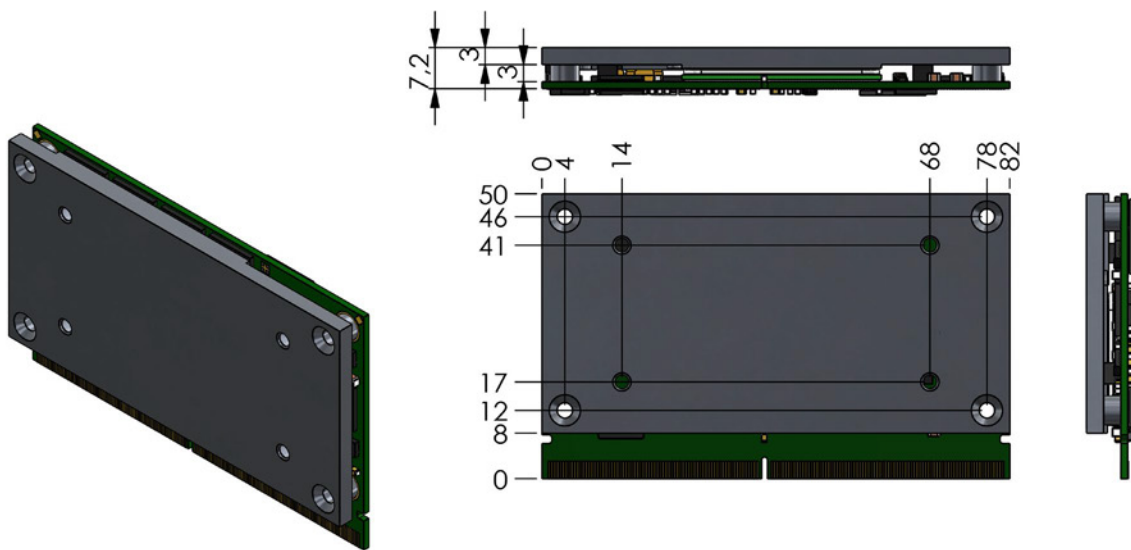




Figure 4: Standard Heat Spreader TQMxE40S-HSP (dimensions in mm)

Attention: Heat Spreader	
	<p>The packages of the Intel® X6000E Series Pentium® and the Intel® X6000E Series Celeron® CPU have a different height than the package of the Intel® X6000E Series Atom™ CPU!</p> <p>The Intel® Atom™ CPU family includes an integrated heat spreader, the Intel® Pentium® and the Intel® Celeron® CPUs have no integrated heat spreaders.</p> <p>Both CPU packages require different heat spreader versions.</p> <p>To mount the wrong heat spreader will damage the TQMxE40S.</p>

Attention: Mounting cooling solution	
	<p>Be careful when selecting the screws for mounting a cooling solution on the heat spreader or fixing the heat spreader in a system. When the screws are too long, they will damage the module by contacting to electronic components or the PCB. The maximum insertion depth of the screws in the TQMxE40S heat spreader is 2.5mm.</p>

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 details about 2D/3D Step models.

4.3 Mechanical and Thermal Considerations

The TQMxE40S 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 TQMxE40S. Therefore, the heat spreader is thermally coupled with the CPU: It ensures an optimal heat transfer from the TQMxE40M 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 TQMxE40S 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 TQMxE40S 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.

4.5 Label placement

TBD



5. SOFTWARE

5.1 System Resources

5.1.1 I²C Bus

The TQMxE40S 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	TQMxE40S EEPROM	–
0xAE	Carrier Board EEPROM	Embedded EEPROM configuration not supported

5.1.2 SMBus

The TQMxE40S provides a System Management Bus (SMBus). On the module there are no SMBus devices.

5.1.3 Memory Map

The TQMxE40S 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 TQMxE40S 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 TQMxE40S 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 TQMxE40S 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 TQMxE40S 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

The TQMxE40S 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>.

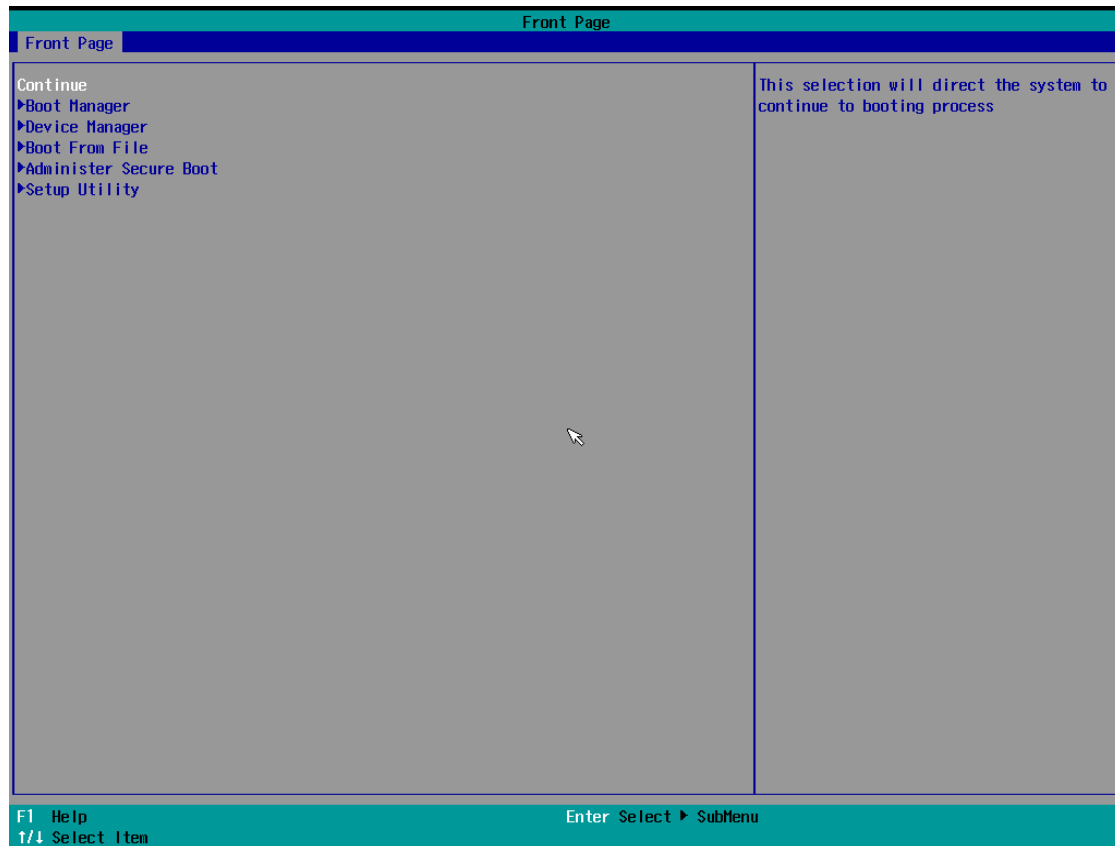


Figure 5: InsydeH2O BIOS Front Page

6.1 Continue Boot Process

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

6.2 Boot Manager

Choose between possible boot options. If system is in UEFI Boot Mode one boot option will 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 to 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 show the option, which can be configured whereas 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 screens 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
Platform Information	See submenu	Shows some platform information.
Language	English / Francis / 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
About this Software	See submenu	Shows Copyright © information of Insyde Software Corp.

6.6.2 Advanced

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

Menu Item	Option	Description
Boot Configuration	See submenu	Configures settings for Boot Phase
USB Configuration	See submenu	Configure USB settings
Chipset Configuration	See submenu	Configure Platform Trust Technology
ACPI Table/Features Control	See submenu	Configure ACPI settings
RC Advanced Menu	See submenu	Configure Reference Code features/settings
SIO TQMx86	See submenu	Configure CPLD UARTs, TQ Board specific configuration and LVDS
Console Redirection	See submenu	Configure console redirection settings
H2OUve Configuration	See submenu	Configure H2OUVE support
SIO F81214E	See submenu	Configure UARTs of Fintek Super I/O F81214E
NVM Express Information	See submenu	Shows NVMe information



6.6.2.1 Boot Configuration

Setup Utility ⇒ Advanced ⇒ Boot Configuration

Menu Item	Option	Description
Numlock	On / Off	Allows to choose whether NumLock Key at system boot must be turned On or Off
Logo & SCU Resolution	Auto / 640 x 480 / 800 x 600 / 1024 x 768	Configuration logo & Setup Utility resolution
Rotate Screen	Disable / 90 degrees clockwise / 270 degrees clockwise	Enable/Disable Rotate Screen feature. Support 90 and 270 degrees clockwise.
H2O Setup – IGD display mode	Text Mode / Graphics Mode	Set the setup display mode for IGD.
H2O Setup – PEG display mode	Text Mode / Graphics Mode	Set the setup display mode for PEG.

6.6.2.2 USB Configuration

Setup Utility ⇒ Advanced ⇒ USB Configuration

Menu Item	Option	Description
USB BIOS Support	Enabled / Disabled	USB keyboard/mouse/storage support under UEFI environment.
Wake on USB from S5	Enabled / Disabled	Enable/Disable Wake on USB from S5 state.

6.6.2.3 Chipset Configuration

Setup Utility ⇒ Advanced ⇒ Chipset Configuration

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

6.6.2.4 ACPI Table/Features Control

Setup Utility ⇒ Advanced ⇒ ACPI Table/Features Control

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



6.6.2.5 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 parameters
Intel® Time Coordinated Computing	See submenu	Intel® Time Coordinated Computing (Intel® TCC) options. This menu shows options and links needed for real time systems.
Memory Configuration	See submenu	Memory configuration parameters
System Agen (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
Thermal Configuration	See submenu	Configure fan speed control under OS and while booting
Platform Settings	See submenu	Platform related settings

6.6.2.5.1 ACPI Settings

Setup Utility ⇒ *Advanced* ⇒ *RC Advanced Menu* ⇒ *ACPI Settings*

Menu Item	Option	Description
Enable ACPI Auto Configuration	[] / [X]	Enables or disabled 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 methods is Direct I/O or ACPI.
ACPI S3 support	Enabled / Disabled	Enable ACPI S3 support.
Native PCIE Enable	Enabled / Disabled	Enable Native PCIE.
Native ASPM	Auto / Enabled / Disabled	Enabled – OS controlled ASPM Disabled – BIOS controlled ASPM
BDAT ACPI Table Support	Enabled / Disabled	Enables support for the BDAT ACPI table
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.

6.6.2.5.2 CPU Configuration

Setup Utility ⇒ *Advanced* ⇒ *RC Advanced Menu* ⇒ *CPU Configuration*

Menu Item	Option	Description
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). Note: Option just configurable when CPU Flex Ratio Override enabled.
Hardware Prefetcher	Enabled / Disabled	To turn on/off the MLC streamer prefetcher.



Menu Item	Option	Description
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 Vanderpool Technology.
Active Processor Cores	All / 1 / 2 / 3	Number of cores to enable in each processor package.
BIST	Enabled / Disabled	Enable/Disable BIST (Built-In Self Test) on reset.
AES	Enabled / Disabled	Enable/Disable AES (Advanced Encryption Standard).
Machine Check	Enabled / Disabled	Enable/Disable Machine Check.
MonitorMWait	Enabled / Disabled	Enable/Disable MonitorMWait.

6.6.2.5.3 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	GT – power management control options

Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ Power & Performance ⇒ CPU – Power Management Control

Menu Item	Option	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/Disable Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power. RTH is controlled through MSR 1FC bit 20.
Intel® Speed Shift Technology	Enabled / Disabled	Enable/Disable Intel® Speed Shift Technology support. Enabling will expose the CPPC v3 interface to allow for hardware controlled P-states.
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/Disable processor Turbo Mode (requires EMTTM enabled too).
View/Configure Turbo Options	See submenu	View/Configure Turbo Options.
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/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. Note: Only shown when C States enabled.



Menu Item	Option	Description
C-State Auto Demotion	C1 / Disabled	Configure C-State Auto Demotion. Note: Only shown when C States enabled.
C-State Un-demotion	C1 / Disabled	Configure C-State Un-demotion. Note: Only shown when C States enabled.
Package C-State Demotion	Enabled / Disabled	Package C-State Demotion. Note: Only shown when C States enabled.
Package C-State Un-demotion	Enabled / Disabled	Package C-State Un-demotion. Note: Only shown when C States enabled.
CState Pre-Wake	Enabled / Disabled	Disable – Sets bit 30 of POWER_CTL MSR(0x1FC) to 1 to disable the Cstate Pre-Wake. Note: Only shown when C States enabled.
IO MWAIT Redirection	Enabled / Disabled	When set, will map IO read instructions sent to IO registers PMG_IO_BASE_ADDRESS+offset to MWAIT(offset). Note: Only shown when C States enabled.
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. Note: Only shown when C States enabled.
Time Unit	1 ns / 32 ns / 1024 ns / 32768 ns / 1048576 ns / 33554432 ns	Unit of measurement for IRTL value – bits [12:10] Note: Only shown when C States enabled.
Latency	0 – 1023	Interrupt Response Time Limit value-bits [9:0]
Thermal Monitor	Enabled Disabled	Enable/Disable thermal monitor.
CPU Lock Configuration	See submenu	CPU Lock configuration

Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ Power & Performance ⇒ CPU – Power Management Control ⇒ View/Configure Turbo Options

Menu Item	Option	Description
Energy Efficient P-state	Enabled / Disabled	Enable/Disable Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 ECX[3] will read 0 indicating no support for Energy Efficient policy setting. When set to 1 will enable access to ENERGY_PERFORMANCE_BIAS MSR 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 1	[X]	Power Limit 1 in milliwatt. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500.



Menu Item	Option	Description
		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 will program TDP value. Note: Option only shown when Power Limit 1 enabled.
Power Limit 1 Time Window	<X>	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 is default value (28 s for Mobile and 8 s for Desktop). Defines time window which TDP value should be maintained. Note: Option only shown when Power Limit 1 enabled.
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 2.
Power Limit 2	[X]	Power Limit 2 in milliwatt. BIOS will round to the nearest 1/8W when programming. If the value is 0, BIOS will program this value as 1.25*TDP. For 12.5W, enter 12500. Processor applies control policies such that the package power does not exceed this limit. Note: Option only shown when Power Limit 2 enabled.
1-Core Ratio Limit Override	[X]	1-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 1-Core Ratio Limit must be greater than or equal to 2-Core Ratio Limit, 3-Core Ratio Limit, 4-Core Ratio Limit
2-Core Ratio Limit Override	[X]	2-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 2-Core Ratio Limit must be greater than or equal to 1-Core Ratio Limit.
3-Core Ratio Limit Override	[X]	3-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 3-Core Ratio Limit must be greater than or equal to 1-Core Ratio Limit.
4-Core Ratio Limit Override	[X]	4-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 4-Core Ratio Limit must be greater than or equal to 1-Core Ratio Limit.
Energy Efficient Turbo	Enabled / Disabled	Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overclocking situations where turbo frequency must remain constant. Otherwise, leave enabled.

Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ Power & Performance ⇒ CPU – Power Management Control ⇒ CPU Lock Configuration

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

Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ Power & Performance ⇒ GT – Power management Control

Menu Item	Option	Description
RC6(Render Standby)	Enabled / Disabled	Check to enable render standby support.
Maximum GT frequency	Default Max Frequency / X MHz	Maximum GT frequency limited by the user. Choose between 200 MHz (RPN) and 400 MHz (RPO). 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



6.6.2.5.4 Intel® Time Coordinated Computing

Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ Intel® Time Coordinated Computing

Menu Item	Option	Description
Intel® TCC Mode	Enabled / Disabled	Enable or Disable Intel® TCC mode. When enabled, this will modify system settings to improve real-time performance. The full list of settings and their current state are displayed below when Intel® TCC mode is enabled.
IO Fabric Low Latency	Enabled / Disabled	Enable or Disable IO Fabric Low Latency. This will turn off some power management in the PCH IO fabrics. This option provides the most aggressive IO Fabric performance setting. S3 state is NOT supported!
GT CLOS	Enabled / Disabled	Enable or Disable Graphics Technology (GT) Class of Service. Enable will reduce Gfx LLC allocation to minimize Impact of Gfx workload on LLC.

All other options are internal links to configurations which could impact to Time Coordinated Computing.

6.6.2.5.5 Memory Configuration

Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ Memory Configuration

Menu Item	Option	Description
REFRESH_2X_MODE	Disabled / 1-Enabled for WARM or HOT 2- Enabled HOT only	0 – Disabled 1 – iMC enables 2xRef when Warm and Hot 2 – iMC enables 2xRef when Hot
In-Band ECC	Enabled / Disabled	Enable/Disable In-Band ECC

6.6.2.5.6 System Agent (SA) Configuration

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

Menu Item	Option	Description
Graphics Configuration	See submenu	Graphics Configuration
VT-d	Enabled / Disabled	VT-d capability
X2APIC Opt Out	Enabled / Disabled	Enable/Disable X2APIC_OPT_OUT bit.
DMA Control Guarantee	Enabled / Disabled	Enable/Disable DMA_CONTROL_GUARANTEE bit.
IGD VTD Enable	Enabled / Disabled	Enable/Disable IGD VTD.
IOP VTD Enable	Enabled / Disabled	Enable/Disable IOP VTD.
GNA Device (B0:D8:F0)	Enabled / Disabled	Enable/Disable SA GNA Device.
CRID Support	Enabled / Disabled	Enable/Disable SA CRID and TCSS CRID control for Intel SIPP.
Above 4GB MMIO BIOS assignment	Enabled / Disabled	Enable/Disable above 4 GB MemoryMappedIO BIOS assignment. This is enabled automatically when Aperture Size is set to 2048 MB.

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

Menu Item	Option	Description
Skip Scanning of External Gfx Card	Enabled / Disabled	If Enabled, it will not scan for External Gfx Card on PEG and PCH PCIE Ports.
Primary Display	Auto / IGD / PCIe	Select which of IGD or 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.



Menu Item	Option	Description
GTT Size	2MB / 4MB / 8MB	Select the GTT Size.
Aperture Size	128MB / 256MB / 512MB / 1024MB / 2048MB	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
DVMT Pre-Allocated	64M / 96M / 128M / 160M / 192M / 224M / 256M / 288M / 320M / 352M / 384M / 416M / 448M / 480M / 512M	Select DVMT5.0 (Dynamic Video Memory Technology) Pre-Allocated (fixed) Graphics Memory size used by the Internal Graphic Device.
DVMT Total Gfx Mem	128M / 256M / MAX	Select the DVMT5.0 (Dynamic Video Memory Technology) Total Graphics Memory size used by the Internal Graphics Device.
DiSM Size	0GB / 1GB / 2GB / 3GB / 4GB / 5GB / 6GB / 7GB	DiSM Size for 2LM Sku.
Intel Graphics Pei Display Peim	Enabled / Disabled	Enable/Disable Pei (Early) Display.
VDD Enable	Enabled / Disabled	Enable/Disable forcing of VDD in the BIOS.
PM Support	Enabled / Disabled	Enable/Disable PM Support.
PAVP Enable	Enabled / Disabled	Enable/Disable PAVP.
Cdynmax Clamping Enable	Enabled / Disabled	Enable/Disable Cdynmax Clamping.
Cd Clock Frequency	307.2 MHz / 556.8 MHz / 652 MHz / Max CdClock freq basen on Reference Clk	Select the highest Cd Clock frequency supported by the platform.
Skip Full CD Clock Init	Enabled / Disabled	Enabled: Skip Full CD clock initialization. Disabled: Initialize the full CD clock if not initialized by Gfx PEIM.
LCD Control	See submenu	LCD Control options.

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	VBIOS Default / 640 × 480 LVDS / 800 × 600 LVDS / 1024 × 768 LVDS / 1280 × 1024 LVDS / 1400 × 1050 LVDS1 / 1400 × 1050 LVDS2 / 1600 × 1200 LVDS / 1366 × 768 LVDS / 1680 × 1050 LVDS / 1920 × 1200 LVDS / 1440 × 900 LVDS / 1600 × 900 LVDS / 1024 × 768 LVDS / 1280 × 800 LVDS / 1920 × 1080 LVDS / 2048 × 1536 LVDS / 1366 × 768 LVDS	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	Back Light Control Setting.



6.6.2.5.7 PCH-IO Configuration

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

Menu Item	Option	Description
PCI Express Configuration	See submenu	PCI Express Configuration settings
SATA configuration	See submenu	SATA device options settings
USB Configuration	See submenu	USB Configuration settings
Security Configuration	See submenu	Security Configuration settings
HD Audio Configuration	See submenu	HD Audio subsystem configuration settings
SCS Configuration	See submenu	Storage and Communication Subsystem (SCS) configuration
PSE Configuration	See submenu	Programmable Service Engine (PSE) configuration
TSN GBE Configuration	See submenu	Time Sensitive Network GBE configuration
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 / Last State	Specify what state to go to when power is re-applied after a power failure (G3 state).
Pcie Pll SSC	Auto / X% / Disable	Pcie Pll SSC percentage. Auto – Keep HW default, no BIOS override Range is 0.0% - 2.0%
Flash Protection Range Registers (FPRR)	Enabled / Disabled	Enable Flash Protection Range Registers.
Global Reset Three Strike Counter	Enabled / Disabled	Enable/Disable Three Strike Counter (if enabled, PMC will keep platform in S5 after 3 rd consecutive type7 global reset occurs during boot flow).

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.
Peer Memory Write Enable	Enabled / Disabled	Peer Memory Write 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 0 th is enabled, 0 th will become visible.
PCIe EQ settings	See submenu	This form contains options for controlling PCIe EQ process.
PCI Express Root Port X	See submenu	Configuration of the corresponding PCI Express Root Port X.

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.
PCIe EQ method	PCIe hardware EQ / PCIe fixed EQ	Choose PCIe EQ method
PCIe EQ mode	Use presets during EQ / Use coefficients during EQ	Choose EQ mode. Preset mode – root port will use presets during EQ process Coefficient mode – root port will use coefficients during EQ process
EQ PH1 downstream port transmitter preset	0 – 10	Choose the value of the preset that will be used during phase 1 of the equalization
EQ PH1 upstream port	0 – 10	Choose the value of the preset that will be used during phase 1 of the



Menu Item	Options	Description
transmitter preset		equalization
Enable EQ phase 2 local transmitter override	[] / [X]	EQ Phase 2 local transmitter override can be used to debug issues with PCI devices equalization
EQ Phase 2 local transmitter override preset	0 – 10	Select preset which will be used during phase 2 of the PCIe EQ process
Number of presets of coefficients used during phase 3	0 – 11	Select how many presets or coefficients will be used during phase 3 of EQ. Please note that you have to set all of the list entries to valid values. The interpretation of this field depends on PCIe EQ mode.
Prese X	0 – 63	Choose the target preset value.

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 / L0s / L1 / L0sL1 / Auto	PCI Express Active State Power Management settings.
L1 Substates	Disabled / L1.1 / L1.1 & L1.2	PCI Express L1 Substates settings.
ACS	Enabled / Disabled	Enable or Disable Access Control Services Extended Capability.
PTM	Enabled / Disabled	Enable or Disable Precision Time Measurement.
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.
SENFEE	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 IO	[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.



Menu Item	Options	Description
		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.
Force LTR Override	Enabled / Disabled	Force LTR Override for PCH PCIE. Disabled: LTR Override values will not be forced. Enabled: LTR override values will be forced and LTR messages from the device will be ignored.
LTR Lock	Enabled / Disable	PCIE LTR configuration lock.

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 / Intel RST Premium With Intel Optane System Acceleration	Determine how SATA controller(s) operate.
SATA Ports Multiplier	Enabled / Disabled	Ports Multiplier enable/disable.
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.
Serial ATA 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.
SATA Port X RxPolarity	Enabled / Disabled	Enable/Disable SATA Port X RxPolarity. Default should disable, please check board design before enable it.
DITO Configuration	Enabled / Disabled	Enable or disable DITO Configuration.
DITO Value	0 – 999	DITO Value. <u>Note:</u> This option is only configurable if "DITO Configuration" is Enabled.
DM Value	0 – 15	DM Value. <u>Note:</u> This option is only configurable if "DITO Configuration" is Enabled.



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

Menu Item	Options	Description
XHCI Compliance Mode	Enabled / Disabled	Option to enable Compliance Mode. Default is to disable Compliance Mode. Change to enabled for Compliance Mode testing.
xDCI Support	Enabled / Disabled	Enable/Disable xDCI (USB OTG Device)
USB Port Disable Override	Select per Pin / Disabled	Selectively enable/disable the corresponding USB port from reporting a Device Connection to the controller.
USB HS / SS Physical Connector #X	Enabled / Disabled	Enable/Disable USB Physical Connector #X (Physical port). Once disabled, any USB device plug into the connector will not be detected by BIOS or OS.
USB Device/HOST Mode Override	Select Per-Pin / Disabled	Selectively Enable/Disable the corresponding USB 2.0 and USB 3.0 device mode.
USB HS / SS X Operation Mode	Platform-POR / USB Host Mode / USB Device Mode	Select USB Operation Mode.

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.

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.
Audio DSP Compliance Mode	Non-UAA (IntelSST) / UAA (HAD Inbox/IntelSST)	Specifies DSP enabled system compliance. Non-UAA (IntelSST driver support only – CC_040100) UAA (HD Audio Inbox or IntelSST driver support – CC_040380)
Audio Link Mode	HD Audio Link / Advanced Link Config	Select Link mode
HDA-Link Codec Select	Platform Onboard / External Kit	Selects whether Platform Onboard Codec (single Verb Table Installed) or External Codec Kit (multiple Verb Tables Installed) will be used.

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

Menu Item	Options	Description
eMMC 5.0 Controller	Enabled / Disabled	Enable or disable SCS eMMC 5.0 Controller.
eMMC 5.1 HS400 Mode	Enabled / Disabled	Enable or disable SCS eMMC 5.1 HS400 Mode in BIOS and OS.
Driver Strength	33 Ohm / 40 Ohm / 50 Ohm	Sets I/O driver strength.
SD card 3.0 Controller	Enabled / Disabled	Enable or disable SCS SDMC 3.0 Controller.



Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ PCH-IO Configuration ⇒ PSE Configuration

Menu Item	Options	Description
PSE Controller	Enabled / Disabled	Enables/Disables Programmable Service Engine (PSE) device
CAN0	None / PSE owned with pin muxed / Host owned with pinx muxed	Enables/Disables CAN interface. PSE owned – CAN used over PSE under Zephyr OS Host owned – CAN used under other OS (Linux)
CAN1	None / PSE owned with pin muxed / Host owned with pinx muxed	Enables/Disables CAN interface. PSE owned – CAN used over PSE under Zephyr OS Host owned – CAN used under other OS (Linux)

Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ PCH-IO Configuration ⇒ TSN GBE Configuration

Menu Item	Options	Description
PCH TSN LAN Controller	Enabled / Disabled	Enable/Disable TSN LAN.
PCH TSN GBE Multi-Vc	Enabled / Disabled	Enable/Disable TSN Multi Virtual Channels.
PCH TSN GBE SGMII Support	Enabled / Disabled	Enable/Disable SGMII mode for PCH TSN GBE. Ports in SGMII mode with the same PLL common lane must use the same link speed. SATA or UFS may need to be disabled if TSN port is using the same PLL common lane. Please make sure IFWI has proper straps set for SGMII. Make sure Flex IO Lane Assignment is not None.
PCH TSN Link Speed	RefClk 24MHz 2.5Gbps / RefClk 24MHz 1Gbps / RefClk 38.4MHz 2.5Gbps / RefClk 38.4MHz 1Gbps /	PCH TSN Link Speed configuration.
PSE TSN GBE X Multi-Vc	Enabled / Disabled	Enable/Disable TSN Multi Virtual Channels. TSN GBE must be host owned.
PSE TSN GBE X SGMII Support	Enabled / Disabled	Enable/Disable Modphy support for SGMII mode for PSE TSN GBE X. Ports in SGMII mode with the same PLL common lane must use the same link speed. UFS will need to be disabled as this TSN port uses the same PLL common lane. Please make sure IFWI has proper straps set for SGMII. Make sure Flex IO Lane Assignment is not NONE.
PSE TSN GBE X Link Speed	RefClk 38.4Mhz 2.5 Gbps / RefClk 38.4Mhz 1Gbps	PSE TSN GBE 0 Link Speed configuration.
Wake on LAN Enable	Enabled / Disabled	Enable/Disable integrated LAN to wake the system.
Skip TSN MAC region	Enabled / Disabled	Skip the TSN MAC region.
Skip TSN IP region	Enabled / Disabled	Skip the TSN IP region.
Skip TSN Config region	Enabled / Disabled	Skip the TSN config region.

6.6.2.5.8 PCH-FW Configuration

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

Menu Item	Option	Description
ME State	Enabled / Disabled	When Disabled ME will be put into ME Temporarily Disabled Mode.
Firmware Update Configuration	See submenu	Configure Management Engine Technology parameters.



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. This option is only valid for next boot.
FW Update	Enabled / Disabled	Enable/Disable ME FW Update function.

6.6.2.5.9 Thermal Configuration

Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ Thermal Configuration

Menu Item	Option	Description
Enable All Thermal Functions	Enabled / Disabled	Enables fan control under OS with different Trip Points.
Platform Thermal Configuration	See submenu	Platform Thermal Configuration options
Hardware Health Monitor	See submenu	Configure Fan speed while boot process.

Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ Thermal Configuration ⇒ Platform Thermal Configuration

Menu Item	Option	Description
Critical Trip Point	15 C – 130 C	This value controls the temperature of the ACPI Critical Trip Point – the point in which the OS will shut the system off. Note: 110 °C is the Plan Of Record (POR) for all Intel mobile processors.
Active Trip Point 0	Disabled / 15 C – 119 C	This value control the temperature of the ACPI Active Trip Point 0 – the point in which the OS will turn the processor fan on Active Trip Point 0 fan speed.
Active Trip Point 0 Fan Speed	0 – 100	Active Trip Point 0 Fan Speed in percentage. Value must be between 0 (fan off) – 100 (max. fan speed). This is the speed at which fan will run when Active Trip Point 0 is crossed.
Active Trip Point 1	Disabled / 15 C – 119 C	This value control the temperature of the ACPI Active Trip Point 1 – the point in which the OS will turn the processor fan on Active Trip Point 1 fan speed.
Active Trip Point 1 Fan Speed	0 – 100	Active Trip Point 1 fan speed in percentage. Value must be between 0 (fan off) – 100 (max. fan speed). This is the speed at which fan will run when Active Trip Point 1 is crossed.
Passive Trip Point	Disabled / 15 C – 119 C	This value controls the temperature of the ACPI Passive Trip Point – the point in which the OS will begin throttling the processor.
Passive TC1 Value	1 – 16	This value sets the TC1 value for the ACPI Passive Cooling Formula.
Passive TC2 Value	1 – 16	This value sets the TC2 value for the ACPI Passive Cooling Formula.
Passive TSP Value	2 – 32	This item sets the TSP value for the ACPI Passive Cooling Formula. It represents in tenths of a second how often the OS will read the temperature when passive cooling is enabled.
Disable Active Trip Points	Enabled / Disabled	Disable Active Trip Points.
Disable Passive Trip Points	Enabled / Disabled	Disable Passive Trip Points.
Disable Critical Trip Points	Enabled / Disabled	Disable Critical Trip Points.

Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ Thermal Configuration ⇒ Hardware Health Monitor

Menu Item	Option	Description
Boot Fan Speed	[0] – [100]	Set the Boot Fan Speed while boot process in percentage.



6.6.2.5.10 Platform Settings

Setup Utility ⇒ Advanced ⇒ RC Advanced Menu ⇒ Platform Settings

Menu Item	Option	Description
HID Event Filter Driver	Enabled / Disabled	Enables/Disables HID Event Filter Driver Interface to OS.
Enable PowerMeter	Enabled / Disabled	Enables/Disables PowerMeter.

6.6.2.6 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.
Power State S5	Normal / Low Power	Configure Power State S5. Normal: Wakeup over LAN (WOL), timer, external wake and power button possible.
GPI Interrupt Configuration	Interrupt disabled / IRQ7 / IRQ9 / IRQ12	Configure the GPI Interrupt number. Note: The interrupt is level high-triggered (ISA-style)!
Gigabit Ethernet SDP	Output – generating time stamp / Input – receive time stamp	Choose if Gigabit Ethernet Software defined Pin (SDP) is used as input (receive time stamp) or output (generating time stamp).
Enable LVDS bridge	Enabled / Disabled	Enable or disable the eDP-to-LVDS bridge.
LVDS Configuration	Enabled / Disabled	Enable or disable the configuration of eDP-to-LVDS bridge.
LVDS Colour depth and data packing format	VESA 24 bpp / JEIDA 24 bpp / VESA and JEIDA 18 bpp	Configure the LVDS Colour depth in eDP-to-LVDS bridge.
LVDS dual/single mode	Single LVDS bus mode / Dual LVDS bus mode	Configure LVDS dual/single mode.
LVDS clock frequency center spreading depth	No Spreading / 0.5 % / 1.0 % / 1.5 % / 2.0 % / 2.5 %	Configure LVDS clock frequency center spreading depth.
LVDS EDID information	EDID Emulation off – read from DDC EDID Emulation on – read from internal Flash	Configure if the EDID information should be read from DDC or internal flash of eDP-to-LVDS bridge.
LVDS Resolution	1024 × 768 @ 60 Hz NXP Generic / 800 × 480 @ 60 Hz NXP Generic / 480 × 272 @ 60 Hz NXP Generic / 1600 × 900 @ 60 Hz Samsung LTM200 KT / 1920 × 1080 @ 60 Hz	Configure the Resolution of eDP-to-LVDS bridge. Note: This option is only visible if 'LVDS EDID information' is set on 'EDID Emulation on – read from internal Flash'.



Menu Item	Option	Description
	Samsung LTM230 HT / 1366 × 768 @ 60 Hz NXP Generic / 320 × 240 @ 60 Hz NXP Generic	

6.6.2.7 Console Redirection

Setup Utility ⇒ Advanced ⇒ Console Redirection

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

If enabled:

Menu Item	Option	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 Post	Yes / No	Console Redirection continue works after POST time.
Text Mode Resolution	AUTO / Force 80x25 / Force 80x24 (DEL FIRST ROW) / Force 80x24 (DEL LAST ROW)	Console Redirection Text Mode resolution. Auto: Follow VGA text mode Force 80x25: Don't care about VGA and force text mode to be 80 x 25 Force 80x24 (DEL FIRST ROW): Don't care about VGA and force text mode to be 80 x 24 and Del first row Force 80x24 (DEL LAST ROW): Don't care about VGA and force text mode to be 80 x 24 and Del last row
AutoRefresh	Enabled / Disabled	When feature enable, screen will be auto refresh once after detect remote terminal was connected.
COM_X	See submenu	Set parameters of serial Port COMX.

Note: All COM / HUART submenu are identical and thus, they just will be listed once.

Menu Item	Option	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.
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.



6.6.2.8 H2OUVE Configuration

Setup Utility ⇒ Advanced ⇒ H2OUVE Configuration

Menu Item	Option	Description
H2OUVE Support	Enabled / Disabled	Enable or disable support for Insyde Tool H2OUVE (UEFI variable editor). This tool is used to change i.e. default values of a BIOS image.

6.6.2.9 SIO F81214E

Setup Utility ⇒ Advanced ⇒ SIO F81214E

Menu Item	Option	Description
UART Port X Configuration	See submenu	UART configuration

Setup Utility ⇒ Advanced ⇒ SIO F81214E ⇒ UART Port X Configuration

Menu Item	Option	Description
UART Port X	Enabled / Disabled	Configure UART port using options: Disabled – Disable device Enabled – Enable device and use below settings
Base I/O Address	3F8h / 2F8h / 3E8h / 2E8h / 338h / 228h / 220h / 238h	System I/O base resources.
Interrupt	IRQ3 / IRQ4 / IRQ5 / IRQ6 / IRQ7 / IRQ10 / IRQ11	System interrupt resources.
Peripheral Type	RS232 / RS485	Choose Port Mode.

6.6.2.10 NVM Express Information

Setup Utility ⇒ Advanced ⇒ NVM Express Information

Information page for NVMe.

6.6.3 Security

Menu Item	Option	Description
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	Option	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.
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	Enabled: Force to enable RTC S5 wake up, even if OS disables it. Support ipwrtest to do RTC S5 wakeup.



Menu Item	Option	Description
CPU Configuration	See submenu	
Wake on PME	Disabled / Enabled by OS / Force Enabled	Determines the action taken when the system power is off and a PCI Power Management Enable (PME) wake up event occurs.

6.6.4.1 CPU Configuration

Setup Utility ⇒ *Power* ⇒ *CPU Configuration*

Menu Item	Option	Description
Bi-directional PROCHOT#	Enabled / Disabled	When a processor thermal sensor trips (either core), the PROCHOT# will be driven. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor.
VTX-2	Enabled / Disabled	Enable or disable the VTX-2 mode support.
VT-d	Enabled / Disabled	Enable or disable VT-d capability. It is recommended to disable IPU when enabling this option. Note: IPU is already disabled and hidden in this BIOS.
TM1	Enabled / Disabled	Enable or disable TM1.
DTS	Enabled / Disabled	Enable or disable Digital Thermal Sensor (DTS).
Active Processor Cores	Enabled / Disabled	Enable this option to disable core in each processor package.
Core 1	Enabled / Disabled	Enable or disable Core 1. This option is hidden when Active Processor Cores is disabled.
Core 2	Enabled / Disabled	Enable or disable Core 2. This option is hidden when Active Processor Cores is disabled.
Core 3	Enabled / Disabled	Enable or disable Core 3. This option is hidden when Active Processor Cores is disabled.
Monitor Mwait	Enabled / Disabled / Auto	Enable or disable Monitor Mwait. If Auto is selected, Monitor Mwait will be disabled for Linux/Yocto OS with B1 silicon. For the rest Monitor Mwait will be enabled.
CPU Power Management	See submenu	

Setup Utility ⇒ *Power* ⇒ *CPU Configuration* ⇒ *CPU Power Management*

Menu Item	Option	Description
Intel® SpeedStep™	Enabled / Disabled	Allows more than two frequency ranges to be supported.
Boot performance mode	Max Performance / Max Battery	Select the performance state that the BIOS will set before OS handoff.
Intel® Turbo Boost Technology	Enabled / Disabled	Enable to automatically allow processor cores to run faster than the base operating frequency if it's operating below power, current and temperature specification limits. Hidden if Intel® SpeedStep™ is disabled.
Power Limit 1 Enable	Enabled / Disabled	Enable or Disable Power Limit 1.
Power Limit 1 Clamp Mode	Enabled / Disabled	Enable or Disable Power Limit 1 Clamp Mode.
Power Limit 1 Power	Auto / 6 – 25	Power Limit 1 in Watt. Auto will program Power Limit 1 based on silicon default support value.
Power Limit 1 Time Window	Auto / 6 -128	Power Limit 1 Time Window Value in Seconds. Auto will program Power Limit 1 Time Window based on silicon default support value.
C-States	Enabled / Disabled	Enable or disable C-States. This option hide corresponding C-States options.
Enhanced C-states	Enabled / Disabled	Enable or disable C1E (Auto halt, low frequency, low voltage). When enabled, CPU will switch to minimum speed when all cores enter C-State. Hidden if C-States is disabled.
Max Package C State	S0ix default / PC2 / C0	This option controls the Max Package C-State that the processor will support. Hidden if C-States is disabled.
Max Core C State	Fused value / Core C10 / Core C9 / Core C8 / Core C7 /	This option controls the Max Core C-State that cores will support. Hidden if C-States is disabled.



Menu Item	Option	Description
	Core C6 / Core C1 / Unlimited	
C-State Auto Demotion	Disabled / C1	Configure C-State Auto Demotion. Hidden if C-States is disabled.
C-State Un-demotion	Disabled / C1	Configure C-State Un-demotion. Hidden if C-States is disabled.

6.6.5 Boot

Menu Item	Option	Description
Boot Type	UEFI Boot Type	Select boot type to Dual type, Legacy type or UEFI type. Note: Operating systems installed in UEFI only will boot in UEFI or Dual boot type, not in Legacy. Also the other way around when an OS is installed in Legacy it will not boot in UEFI type. Note: Only UEFI Boot Type is supported on Elkhart Lake.
Quick Boot	Enabled / Disabled	Allow InsydeH2O to skip certain tests while booting. This will decrease the time needed to boot the system.
Quite Boot	Enabled / Disabled	Enable or disable booting in text mode. No textual outputs are given while booting if this option is disabled.
Network Stack	Enabled / Disabled	Enable or disable Network stack Support: Windows 8 BitLocker Unlock UEFI IPv4/IPv6 PXE Legacy PXE OPROM Note: This option will grey-out the PXE Boot capability option.
PXE Boot capability	Disabled / UEFI: IPv4 / UEFI: IPv6 / UEFI: IPv4/IPv6	Disabled: Support network stack UEFI PXE: IPv4/IPv6 Legacy: Legacy PXE OPROM only
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.
Add Boot Options	First / Last / Auto	Position in boot order for shell, network and removables.
ACPI Selection	Acpi1.0B / Acpi3.0 / Acpi4.0 / Acpi5.0 / Acpi6.0 / Acpi6.1	Select booting to which ACPI version.
USB Boot	Enabled / Disabled	Enable or disable booting to USB boot device.
EFI Device First	Enabled / Disabled	Determine EFI device first or legacy device first. If enable, it is EFI device first. If disable, it is legacy device first.
UEFI OS Fast Boot	Enabled / Disabled	If enabled the system firmware does not initialize keyboard and check for firmware menu key. Note: If enabled it is not possible to change to BIOS menu by pressing <F10> when booting Windows.
USB Hot Key Support	Enabled / Disabled	Enable or disable to support USB hot key while booting. This will decrease the time needed to boot the system, however, it is not possible to get into BIOS menu by pressing <ESC> while booting. The change into BIOS has to be done over OS.
Timeout	0 – 10	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.

6.6.6 Exit

Menu Item	Option	Description
Exit Saving Changes		Save changes and reboot system afterwards. <F10> can be used for this operation.
Save Change Without Exit		Save changes without reboot system.
Exit Discarding Changes		Exit InsydeH2O Setup Utility without saving any changes. <ESC> can be used for this operation.
Load Optimal Defaults		Load optimal default values for all setup items. <F9> can be used for this operation.
Load Custom Defaults		Load custom default values for all setup items.
Save Custom Defaults		Save custom defaults for all setup items.
Discard Changes		Discard all changes without exiting InsydeH2O Setup Utility.

6.7 BIOS Update

The uEFI BIOS update instruction serves to guarantee a proper way to update the uEFI BIOS on the TQMxE40S.

Please read the entire instructions before beginning the BIOS update. By disregarding the information you can destroy the uEFI BIOS on the TQMxE40S!

This document will guide the customer to update the uEFI BIOS on the TQMxE40S by using the Insyde Flash Firmware Tools.

Please contact support@tq-group.com for more information to the latest uEFI BIOS version for the TQMxE40S.

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.

6.7.1 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)
- InsydeH2OFF_x86_WIN folder (Flash Firmware Tool from Insyde for update via Windows 32-bit system)
- InsydeH2OFF_x86_WINx64 folder (Flash Firmware Tool from Insyde for update via Windows 64-bit system)
- BIOS.bin file e.g. xx.bin




6.7.2 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 ⇒ 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.

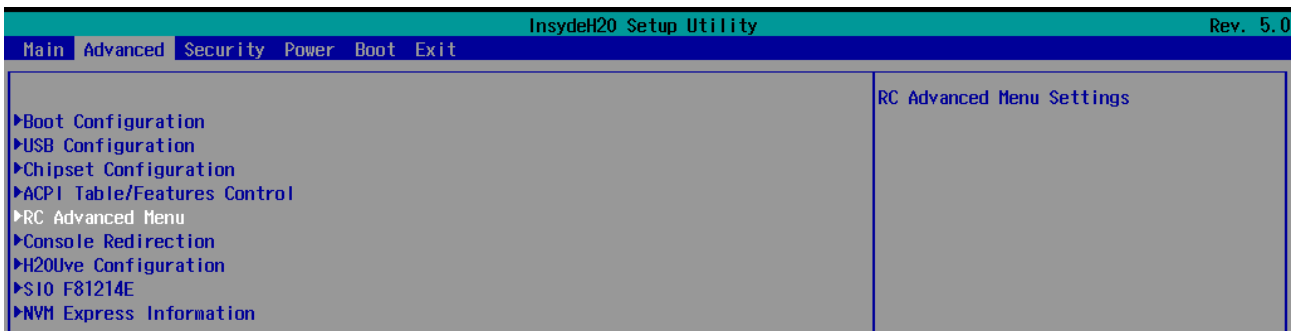


Figure 6: RC Advanced Menu

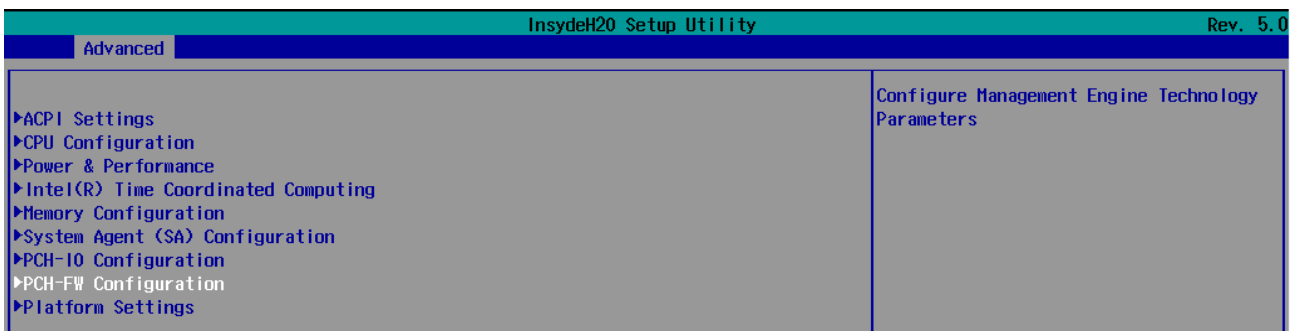


Figure 7: PCH-FW Configuration menu

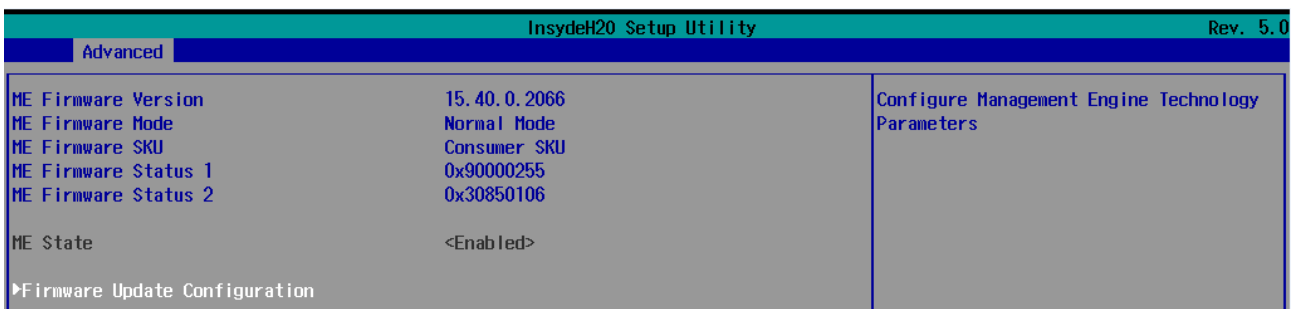


Figure 8: Firmware Update configuration menu

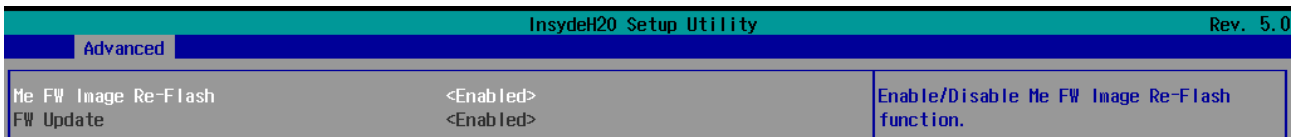


Figure 9: ME FW Image Re-Flash option

6.7.3 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".

```

Mapping table
FS0: Alias(s):HD0d0b0b:;BLK1:
    Pc iRoot(0x0)/Pc i(0x14, 0x0)/USB(0x3, 0x0)/USB(0x1, 0x0)/HD<1, MBR, 0x00000000, 0x2000, 0x1E1D800>
BLK0: Alias(s):
    Pc iRoot(0x0)/Pc i(0x14, 0x0)/USB(0x3, 0x0)/USB(0x1, 0x0)
Shell>
  
```

Figure 10: 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 tqmxe40m") 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.

```

Mapping table
FS0: Alias(s):HD0d0b0b:;BLK1:
    Pc iRoot(0x0)/Pc i(0x14, 0x0)/USB(0x3, 0x0)/USB(0x1, 0x0)/HD<1, MBR, 0x00000000, 0x2000, 0x1E1D800>
BLK0: Alias(s):
    Pc iRoot(0x0)/Pc i(0x14, 0x0)/USB(0x3, 0x0)/USB(0x1, 0x0)
Shell> fs0:
FS0:\> H2OFFT-Sx64.efi TQMxE40M_05.42.43.09.01.bin -all -ra
  
```

Figure 11: EFI Shell uEFI BIOS Update

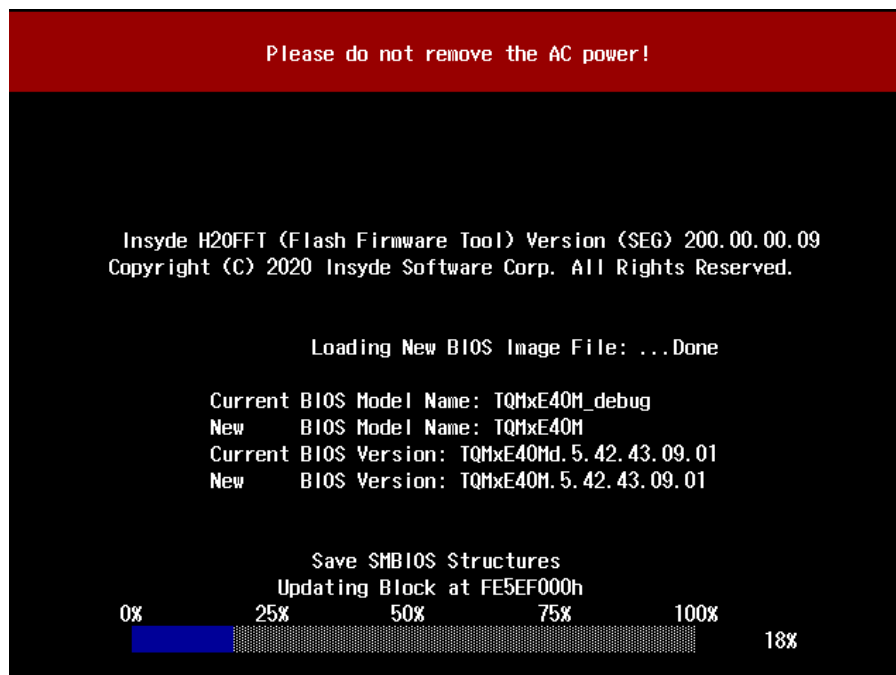


Figure 12: Screen during BIOS Update

6.7.4 Step 2b: Updating uEFI BIOS via Windows Operating System

Boot the Windows operating system (64-bit) and plug the USB stick into the board you want to update the uEFI BIOS. Start the Command prompt (CMD), important 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.

6.7.5 Step 3: BIOS update check on the TQMxE40S Module

After the uEFI BIOS update the new uEFI BIOS configures the complete TQMxE40S hardware and this results in some reboots and the first boot time takes longer (up to 1 – 2 minutes).

The TQMxE40S 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 the uEFI BIOS boot is finished.

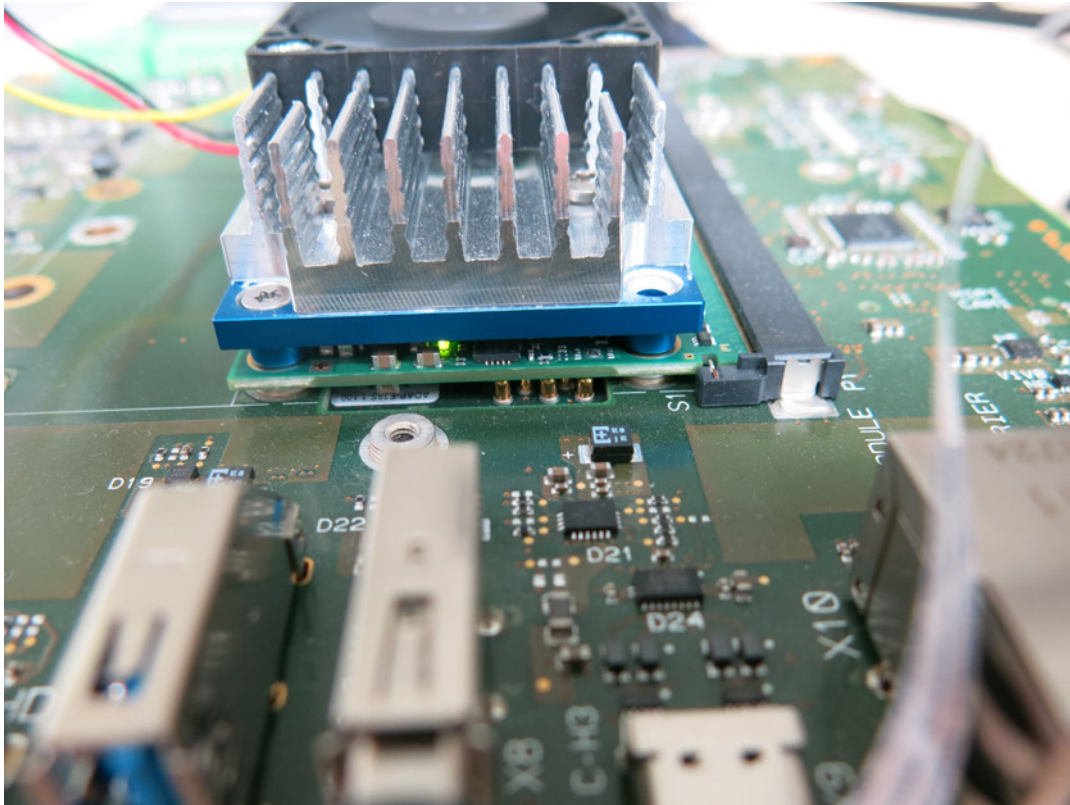


Figure 13: TQMxE40S Debug LED

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.

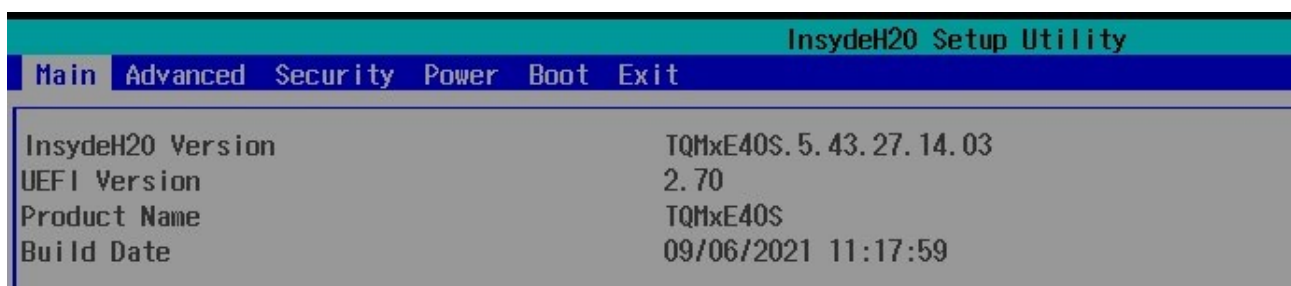


Figure 14: EFI BIOS Main Menu



7. SAFETY REQUIREMENTS AND PROTECTIVE REGULATIONS

7.1 EMC

The TQMxE40S 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.

7.2 ESD

In order to avoid interspersions 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 TQMxE40S.

7.3 Shock & Vibration

The TQMxE40S 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.

7.4 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.

7.5 Reliability and Service Life

The MTBF according to MIL-HDBK-217F N2 is 407 161 hours, Ground Benign, at +40 °C.



8. ENVIRONMENT PROTECTION

8.1 RoHS

The TQMxE40S is manufactured RoHS compliant.

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

8.2 WEEE®

WEEE® regulations do not apply since the TQMxE40S cannot operate on its own.

8.3 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.

8.4 EuP

The Ecodesign Directive, also Energy using Products (EuP), is applicable to products for the end user with an annual quantity >200,000. The TQMxE40S must therefore always be seen in conjunction with the complete device.

The available standby and sleep modes of the components on the TQMxE40S enable compliance with EuP requirements for the TQMxE40S.

8.5 Battery

No batteries are assembled on the TQMxE40S.

8.6 Packaging

By environmentally friendly processes, production equipment and products, we contribute to the protection of our environment. To be able to reuse the TQMxE40S, 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 TQMxE40S is delivered in reusable packaging.

8.7 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.

9. APPENDIX

9.1 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 ² C	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



9.1 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



9.2 References

Table 12: Further Applicable Documents and Links

No.	Name	Rev., Date	Company
(1)	SMARC (Smart Mobility ARChitecture) Hardware Specification	Version 2.1, March 23, 20	SGEI
(2)	SMARC (Smart Mobility ARChitecture) Design Guide	Rev. 2.1.1, April 29, 2021	SGEI

