TQMxE40M
User's Manual

TQMxE40M UM 0102
24.04.2025

TABLE OF CONTENTS

1. ABOUT THIS MANUAL 1
1.1 Copyright and license expenses 1
1.2 Registered trademarks 1
1.3 Disclaimer 1
1.4 Intended Use 1
1.5 Imprint 2
1.6 Service and Support 2
1.7 Tips on safety 2
1.8 Symbols and typographic conventions 2
1.9 Handling and ESD tips 3
1.10 Naming of signals 3
1.11 Further applicable documents / presumed knowledge 3
2. INTRODUCTION 4
2.1 Functional Overview 4
2.2 COM Express™ Specification Compliance 5
2.3 TQMxE40M Variants 5
2.4 Accessories 5
3. FUNCTION 6
3.1 TQMxE40M Block diagram 6
3.2 Electrical characteristics 6
3.2.1 Supply voltage 6
3.2.2 Power consumption 7
3.2.3 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 LPDDR4x 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
3.4.7 Ultra Deep Power State Green ECO-Off 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 12
3.5.5 LVDS Interface 12
3.5.6 USB Interfaces 12
3.5.7 SD Card Interface 12
3.5.8 General Purpose Input / Output 13
3.5.9 High Definition Audio Interface 13
3.5.10 LPC Bus / eSPI 13
3.5.11 I^2C Bus 13
3.5.12 SMBus 13
3.5.13 Serial Peripheral Interface 13
3.5.14 Serial Ports 13
3.5.15 CAN interface 14
3.5.16 Watchdog Timer 14
3.6 Connectors & LEDs 14
3.6.1 COM Express™ Connector 14
3.6.2 Debug Header 14
3.6.3 TQM Debug Card 15
3.6.4 Debug LED 15
3.7 COM Express™ Connector Pinout List 16
3.7.1 Signal Assignment Abbreviations 16
3.7.2 COM Express™ Connector Pin Assignment 17

4. MECHANICS ... 21
4.1 TQMxE40M Dimensions ... 21
4.2 Heat Spreader ... 22
4.3 Mechanical and Thermal Considerations ... 23
4.4 Protection against external effects ... 23
4.5 Label placement ... 23
5. Software ... 25
5.1 System Resources ... 25
5.1.1 I^2C Bus ... 25
5.1.2 SMBus ... 25
5.1.3 Memory Map ... 25
5.1.4 IRQ Map ... 25
5.2 Operating Systems ... 26
5.2.1 Supported Operating Systems ... 26
5.2.2 Driver Download ... 26
5.3 TQ-Systems Embedded Application Programming Interface (EAPI) ... 26
5.4 Software Tools ... 26
6. BIOS ... 27
6.1 Continue Boot Process ... 27
6.2 Boot Manager ... 27
6.3 Device Manager ... 28
6.3.1 Driver Health Manager ... 28
6.3.2 Network Device List ... 28
6.4 Boot from File ... 28
6.5 Administer Secure Boot ... 28
6.6 Setup Utility ... 29
6.6.1 Main ... 29
6.6.2 Advanced ... 29
6.6.2.1 Boot Configuration ... 30
6.6.2.2 USB Configuration ... 30
6.6.2.3 Chipset Configuration ... 30
6.6.2.4 ACPI Table/Features Control ... 30
6.6.2.5 RC Advanced Menu ... 31
6.6.2.6 SIO TQMx86 ... 43
6.6.2.7 Console Redirection ... 44
6.6.2.8 H2OUVE Configuration ... 45
6.6.2.9 SIO F81214E ... 45
6.6.2.10 NVM Express Information ... 46
6.6.3 Security ... 46
6.6.4 Power ... 46
6.6.5 Boot ... 46
6.6.6 Exit ... 47
6.7 BIOS Update ... 47
6.7.1 Step 1: Preparing USB Stick ... 48
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 3b: Updating uEFI BIOS via Windows Operating System ... 50
6.7.5 Step 4: BIOS update check on the TQMxE40M 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 Cyber Security ... 52
7.6 Export Control and Sanctions Compliance ... 52
7.7 Warranty ... 52
7.8 Reliability and service life ... 52
8. ENVIRONMENT PROTECTION ... 53
8.1 RoHS ... 53
8.2 WEEE® ... 53
8.3 REACH® ... 53
8.4 Statement on California Proposition 65 ... 53
8.5 EuP ... 53
8.6 Battery ... 53
8.7 Packaging ... 53

8.8 Other entries 53
9. APPENDIX 55
9.1 Acronyms and definitions 55
9.2 References 57

TABLE DIRECTORY

Table 1: Terms and Conventions 2
Table 2: TQMxE40M Power Consumption 7
Table 3: RTC Power 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: Serial Port COM Express™ Port Mapping 14
Table 8: LED boot messages 15
Table 9: Abbreviations used in Table 10 16
Table 10: COM Express™ Connector Pin Assignment 17
Table 11: Labels on TQMxE40M 23
Table 12: I²C address mapping COM Express™ I²C port 25
Table 13: Acronyms 55
Table 14: Further applicable documents and links 57

ILLUSTRATION DIRECTORY

Illustration 1: Block Diagram TQMxE40M 6
Illustration 2: TQM Debug Card 15
Illustration 3: Three-sided drawing of the TQMxE40M (dimensions in mm) 21
Illustration 4: Bottom view drawing of the TQMxE40M 21
Illustration 5: Standard Heat Spreader 22
Illustration 6: Low-Profile Heat Spreader 22
Illustration 7: Label Placement 24
Illustration 8: InsydeH2O BIOS Front Page 27
Illustration 9: RC Advanced Menu 48
Illustration 10: PCH-FW Configuration menu 48
Illustration 11: Firmware Update Configuration menu 49
Illustration 12: ME FW Image Re-Flash option 49
Illustration 13: EFI Shell 49
Illustration 14: EFI Shell uEFI BIOS Update 49
Illustration 15: Screen during BIOS Update 50
Illustration 16: TQMxE40M Debug LED 51
Illustration 17: EFI BIOS Main Menu 51

REVISION HISTORY

Rev.	Date	Name	Pos.	Modification
0001	19.10.2021	SP		Initial internal release
0100	18.11.2021	Kreuzer		Initial public release
0101	13.12.2021	Kreuzer	3.5.4	Note for HDMI/DVI added
0102	24.04.2025	Kreuzer	1.4, 7.5, 7.6, 7.7, 8.4 3.7	Chapter added Connector source added

1. ABOUT THIS MANUAL

1.1 Copyright and license expenses

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

The drivers and utilities for the components used as well as the BIOS are subject to 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 Intended Use

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

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

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

1.5 Imprint

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

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

1.6 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.

1.7 Tips on safety

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

1.8 Symbols and typographic conventions

Table 1: Terms and Conventions

Symbol	Meaning
	This symbol represents the handling of electrostatic-sensitive modules and / or components. These components are often damaged / destroyed by the transmission of a voltage higher than about 50 V. A human body usually only experiences electrostatic discharges above approximately 3,000 V.
	This symbol indicates the possible use of voltages higher than 24 V. Please note the relevant statutory regulations in this regard. Non-compliance with these regulations can lead to serious damage to your health and 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.

1.9 Handling and ESD tips

General handling of your TQ-products

	The TQ-product may only be used and serviced by certified personnel who have taken note of the information, the safety regulations in this document and all related rules and regulations. A general rule is: do not touch the TQ-product during operation. This is especially important when switching on, changing jumper settings or connecting other devices without ensuring beforehand that the power supply of the system has been switched off. Violation of this guideline may result in damage / destruction of the TQMxE40M and be dangerous to your health. Improper handling of your TQ-product would render the guarantee invalid.

Proper ESD handling

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

1.10 Naming of signals

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

Example: RESET#

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

Example: C / D#

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

The identification of the individual functions follows the above conventions.

Example: WE2# / OE#

1.11 Further applicable documents / presumed knowledge

- **Specifications and manual of the modules used:**
  These documents describe the service, functionality and special characteristics of the module used.
- **Specifications of the components used:**
  The manufacturer's specifications of the components used, 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 COM Express™ Design Guide (2) maintained by the PICMG®. This Carrier Design Guide includes a very good guideline to design a COM Express™ carrier board.

It includes detailed information with schematics and detailed layout guidelines.

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

2. INTRODUCTION

The TQ module TQMxE40M 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 TQMxE40M corresponds to the internationally established PICMG® standard COM Express™ Mini (COM.0 R2.1) with Type10 pinout. 8 USB ports – including 2 USB 3.0 – and up to 4 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 TQMxE40M 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, GPIO handling and "Green ECO-Off" with a minimum of standby power. Combined with options like conformal coating and optimized cooling solutions the TQMxE40M also fits perfectly for mobile, low power, ruggedized 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 TQMxE40M:

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:

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

Peripheral interfaces:

- 1 × Gigabit Ethernet (Marvell 88E1512)
- 2 × USB 3.2 (with up to 10 Gb/s and USB 2.0 backward compatibility)
- 8 × USB 2.0 (incl. USB 3.0 ports)
- 2 × SATA 3.0 (up to 6 Gb/s), eSATA capable
- 4 × PCIe Gen 3 (up to 8 GT/s)
- 1 × LPC bus or eSPI interface
- 1 × Intel® HD audio (HDA)
- 1 × I²C, (2nd I²C optional) (master/slave capable)
- 1 × SMBus
- 1 × SPI (for external uEFI BIOS flash)
- 2 × Serial port (Rx/Tx, legacy compatible), 4 wire optional through TQ-flexiCFG
- 1 × CAN interface (multiplexed with serial port 1)
- 1 × SD card interface / optional 8 × GPIO through TQ-flexiCFG (multiplexed, configurable in BIOS menu)

Security components:

- TPM (SLX9670 TPM 2.0)

Others:

- TQMx86 board controller with watchdog and TQ-flexiCFG

Power supply:

- Voltage: 4.75 V to 20 V
  5 V standby (optional)
  3 V battery for RTC

Environment:

- Standard temperature: 0 °C to +60 °C
- Extended temperature: –40 °C to +85 °C

Form factor / dimensions:

- COM Express™ Mini, Type10; 84 mm × 55 mm

2.2 COM Express™ Specification Compliance

The TQMxE40M is compliant to the PICMG® COM Express™ Module Base Specification (COM.0 R3.0) Mini, Type10, with dimensions of 84 mm × 55 mm.

2.3 TQMxE40M Variants

The TQMxE40M is available in several standard configurations:

Please visit www.tq-group.com/TQMxE40M for a complete list of standard versions.
Other configurations are available on request.

Standard configuration features are:

- eDP or single 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

TQMxE40M-HSP-AB (11 mm): Heat spreader for TQMxE40M according to the COM Express™ specification
TQMxE40M-HSP-AA (6 mm): Heat spreader for TQMxE40M, low profile for designs with very low heights
Evaluation platform MB-COME10-2:

- Mainboard for COM Express™ Mini modules, Type10
- 170 mm × 170 mm
- Interfaces: DP, eDP/LVDS, GbE, 2.5 GbE, 6x USB (1x Type C, 1x USB3.0 Type A, 2x USB 2.0 Type A, 2x int. connector), Audio, several COM ports, CAN, M.2 (Key A, B, M), PCIe socket, µSD card socket, SATA connector

3. FUNCTION

3.1 TQMxE40M Block diagram

The following illustration shows the block diagram of the TQMxE40M:

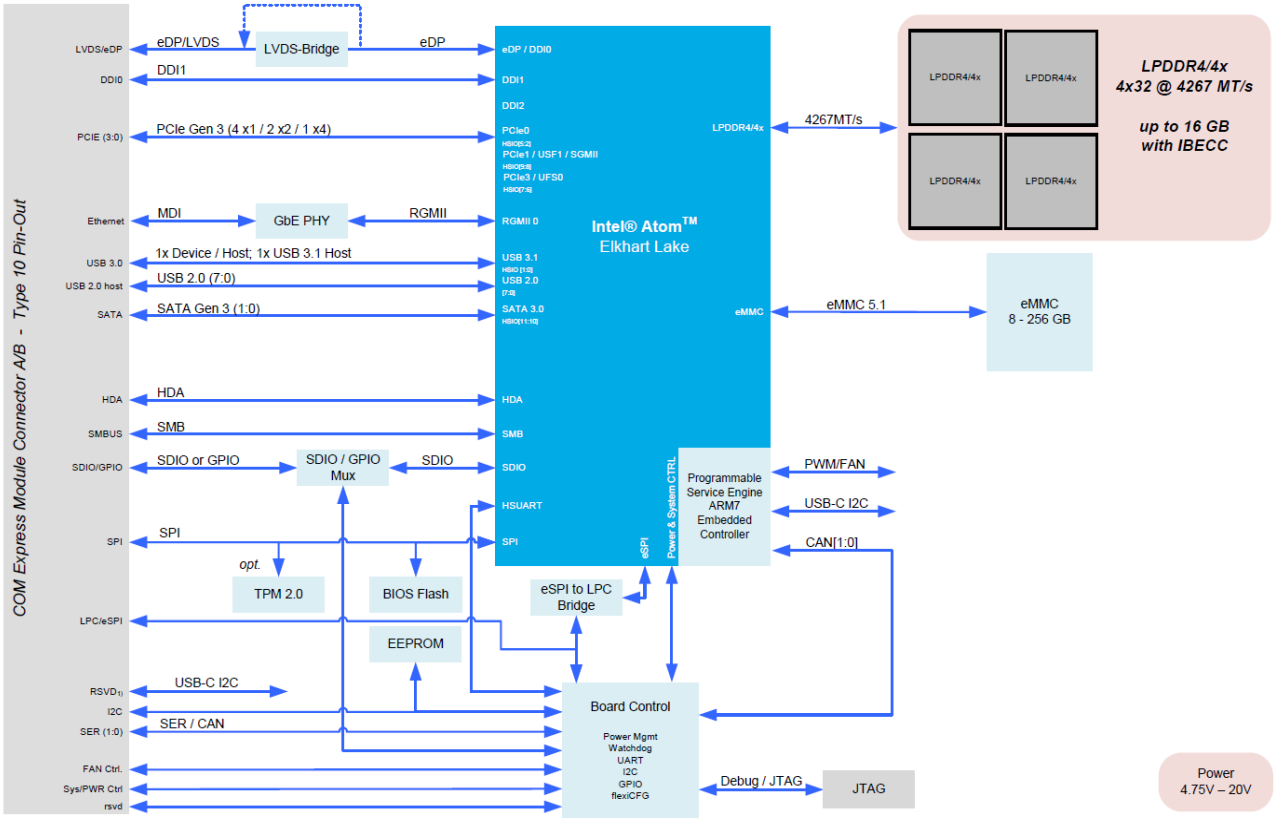


Illustration 1: Block Diagram TQMxE40M

3.2 Electrical characteristics

3.2.1 Supply voltage

The TQMxE40M supports a wide-range voltage input from 4.75 V to 20.0 V DC.

The following supply voltages are specified at the COM Express™ connector:

- Wide input: 4.75 V to 20.0 V max input ripple: ±100 mV
- VCC_5V_SBY: 4.75 V to 5.25 V max input ripple: ±50 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 95 % of nominal within 0.1 ms 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.

Note: Power source	
	For single supply operations, the 5 V Standby voltage is not required. VCC_5V_SBY can be left unconnected.

3.2.2 Power consumption

The values given below show the voltage and power consumption of the TQMxE40M. They were measured using the TQMxE40M and the MB-COME10-2 COM Express™ carrier board.

The measurement was done with two power supplies, one for the TQMxE40M and the other one for the MB-COME10-2 COM Express™ carrier board.

The power consumption of each TQMxE40M 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 +12.0 V.

The power consumption of the TQMxE40M depends on the application, the mode of operation and the operating system.

The power consumption was measured under the following conditions:

- **Green ECO-Off state:**
  The system is in Green ECO-Off state, all DC/DC power supplies on the TQMxE40M are off.
- **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: TQMxE40M Power Consumption

CPU on TQMxE40M	Mode			
	Standby 5 V		Input 5.0 V	
	Green ECO-Off state	Suspend	Win10, 64 bit idle	Win10, 64 bit max. load
SKU6 Atom® x6413E	7.0 mW	1.04 W	5.6 W	11.2 W
SKU7 Atom® x6425E	7.0 mW	1.04 W	5.9 W	14.5 W
SKU8 Atom® x6212RE	7.0 mW	1.04 W	5.0 W	8.2 W
SKU9 Atom® x6425RE	7.0 mW	1.04 W	5.5 W	11.1 W
SKU10 Atom® x6425RE	7.0 mW	1.04 W	5.9 W	14.3 W

Note: Power requirement	
	The power supplies on the carrier board for the TQMxE40M must be designed with enough reserve. The carrier board should provide at least twice the maximum workload power of the TQMxE40M. The TQMxE40M supports several low-power states. The power supply of the carrier board has to be stable even with no load.

3.2.3 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 Power 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 TQMxE40M 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 TQMxE40M supports the Intel® X6000E Series.
The following list shows some key features of these CPUs:

- Quad and dual CPU cores with up to 3 GHz
- 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 (only two are supported by TQMxE40M due to COM Express™ Type 10 limitations)

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 (except x6200FE). 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 TQMxE40M supports one Digital Display Interface (DDI0) and one eDP or single LVDS interface at the COM Express™ connector.

Table 5: Maximum Resolution

Display	Maximum display resolution
LVDS	1400 × 1050 at 60 Hz (single channel)
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 LPDDR4x SDRAM

The TQMxE40M supports a memory-down 4 x 32 bit LPDDR4x configuration running at up to 4267 MT/s and optional In Band ECC (IBECC). The maximum memory size is 16 Gbyte. The available memory configuration can be either 4 Gbyte, 8 Gbyte, or 16 Gbyte.

3.4.3.2 eMMC

The TQMxE40M 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	
	The on-board eMMC Flash requires pre-configuration via EFI Shell before OS installation (e.g. diskpart utility)

3.4.3.3 SPI Boot Flash

The TQMxE40M 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.
The uEFI BIOS supports the following 3.3 V SPI flash devices on the carrier board: Macronix MX25L25645GM2I-08G

3.4.3.4 EEPROM

The TQMxE40M supports a COM Express™ Module EEPROM. The 32 Kbit (24AA32AT) EEPROM is connected to the general purpose I^2C interface (COM Express™ pin names I2C_DAT and I2C_CK).

3.4.4 Real Time Clock

The TQMxE40M includes a standard RTC (Motorola MC146818B) integrated in the Intel® X6000E Series CPU.

3.4.5 Trusted Platform Module

The TQMxE40M 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 TQ-Systems COM Express™ module includes a flexible I/O configuration feature, the TQ-flexiCFG.
Using the TQ-flexiCFG feature, several COM Express™ 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 TQMxE40M 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, CAN, I^2C, PWM controller or special power management configurations

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

3.4.7 Ultra Deep Power State Green ECO-Off

The TQMxE40M supports the ultra-deep power state Green ECO-Off.
In this configuration all DC/DC power supplies on the TQMxE40M are switched off.
This results in lowest power consumption. The Green ECO-Off mode can be configured in the uEFI BIOS setup.
To wake up the system from the Green ECO-Off mode, the power button signal must be pulled low for a minimum of 100 ms.

3.5 Interfaces

3.5.1 PCI Express

The TQMxE40M with Intel® X6000E Series CPU supports a very flexible PCI Express configuration with up to 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 TQMxE40M provides the Marvell 88E1512 Ethernet PHY with 10/100/1000 Mbps speed.
The Ethernet LED functionality defined in the COM Express™ specification is currently not supported by the TQMxE40M module. Intel is working on this issue.

3.5.3 Serial ATA

The TQMxE40M supports two SATA Gen 3.0 (6 Gbit/s) interfaces.
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 TQMxE40M supports two Digital Display Interfaces (DDI0 & DDI1) at the COM Express™ connector.
The DDI0 port supports DisplayPort or HDMI/DVI.
The DDI1 port supports LVDS (via an eDP to LVDS bridge) or eDP as an assembly option.

The TQMxE40M 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

For an HDMI/DVI output, a level converter must be used on the carrier board.

Please contact support@tq-group.com for further information about the DDI0 / DDI1 configuration.

3.5.5 LVDS Interface

The TQMxE40M supports a single channel LVDS interface at the COM Express™ connector.
The LVDS interface is provided through an on-board eDP to LVDS bridge. This bridge supports single LVDS signalling only with colour depths of 18 bits per pixel or 24 bits per pixel up to 112 MHz and a resolution up to 1400 × 1050 at 60 Hz in single 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 Interfaces

The TQMxE40M supports eight USB 2.0 and two USB 3.2 Gen2 ports with data rate up to 10 Gb/s at the COM Express™ connector.
The USB SuperSpeed ports are configured to USB 3.2 Gen1 (5 Gb/s) per default.
Care must be taken in the COM Express™ carrier design, the carrier has to support the USB 3.2 Gen2 (10 Gb/s) high speed standard if this mode is needed.

Attention: USB 3.1 Gen 2 (10 Gb/s) carrier design	
	The COM Express™ specification Revision 3.0 only supports the USB 3.2 Gen1 (5 Gb/s) data rate. If the COM Express™ carrier is not designed for the USB 3.2 Gen2 (10 Gb/s) operation, the USB 3.2 ports should be configured to operate in Gen1 mode.

Please contact support@tq-group.com for further information about USB 3.1 high-speed Design Guidelines.

Note: USB Port Mapping	
	The USB 2.0 port 0 must be paired with USB 3.2 SuperSpeedPlus port 0. The USB 2.0 port 1 must be paired with USB 3.2 SuperSpeedPlus port 1.

3.5.7 SD Card Interface

The TQMxE40M provides an SD card interface for 4-bit SD/MMC cards at the COM Express™ connector. However the SD card signals are shared with the GPIO signals and can be configured via an uEFI BIOS setting. The default configuration at the COM Express™ connector is GPIO and the SD Card interface is not activated in BIOS default settings.

3.5.8 General Purpose Input / Output

The TQMxE40M provides eight GPIO signals at the COM Express™ connector. However the GPIO signals are shared with the SD card signals and can be configured via an uEFI BIOS setting. The default configuration at the COM Express™ connector is GPIO.

The GPIO signals are integrated in the TQ-flexiCFG block and can be flexible configured. Therefore the signals can also be used for several special functionality (see 3.4.7).

3.5.9 High Definition Audio Interface

The TQMxE40M provides a High Definition Audio (HDA) interface, which supports an audio codec at the COM Express™ connector. On the COM Express™ connector there is no HDA_SDIN2 signal available.

3.5.10 LPC Bus / eSPI

The TQMxE40M provides a Low Pin Count (LPC) legacy bus and the Enhanced Serial Peripheral eSPI bus on the same COM Express™ connector pins.

The LPC bus is a 3.3V bus and eSPI is a 1.8V bus. There is the possibility of a mismatch an eSPI only module mated with a LPC only carrier, or an LPC only module on an eSPI carrier!
The TQMxE40M includes a multiplexer that switches between the LPC bus and the eSPI bus on the COM Express™ connector pins.
With the ESPI_EN# signal the carrier indicate the operating mode of the LPC / eSPI bus. If left unconnected on the carrier, LPC mode (default) is selected. If pulled to GND on the carrier, eSPI mode is selected.

Note: LPC / eSPI bus	
	Starting with the Intel® Atom® X6000E Series, the legacy Low Pin Count (LPC) interface has been removed from the processor silicon. The TQMxE40M module includes an eSPI to LPC bridge to support the LPC legacy bus. For new carrier designs the Enhanced Serial Peripheral eSPI bus should be selected.

3.5.11 I²C Bus

The TQMxE40M provides a general purpose I²C port 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.

3.5.12 SMBus

The TQMxE40M provides a System Management Bus (SMBus).

3.5.13 Serial Peripheral Interface

The TQMxE40M provides an SPI interface. The SPI interface can only be used for SPI boot Flash devices.

3.5.14 Serial Ports

The TQMxE40M offers a dual Universal Asynchronous Receiver and Transmitter (UART) controller. The register set is based on the industry standard 16550 UART. The UART operates with standard serial port drivers without requiring a custom driver to be installed. The 16 byte transmit and receive FIFOs reduce CPU overhead and minimize the risk of buffer overflow and data loss.

With the TQ-flexiCFG feature the serial ports can be configured to route the handshake signals to free pins at the COM Express™ connector.

Table 7: Serial Port COM Express™ Port Mapping

COM Express™ Signal	COM Express™ Pin	TQMxE40M	Remark
SER0_TX	A98	SER0_TX	3.3 V output
SER0_RX	A99	SER0_RX	3.3 V input
SER1_TX	A101	SER1_TX	3.3 V output
SER1_RX	A102	SER1_RX	3.3 V input
SER0_RTS#	B77	SER0_RTS#	3.3 V output
SER0_CTS#	B78	SER0_CTS#	3.3 V input
SER1_RTS#	B91	SER1_RTS#	3.3 V output
SER1_CTS#	B92	SER1_CTS#	3.3 V input

Note: Protection circuits	
	In Revision 2.1 of the COM Express™ specification, the signals A98, A99, A101 and A102 have been reclaimed from the VCC_12V pool. Therefore protection on the carrier board is necessary to avoid damage to those when accidentally connected to 12 V. The implementation of this circuitry causes lower transfer rates at both serial ports. On the TQMxE40M the protection circuit is removed by default and the serial ports provide transfer rates of up to 115 kbaud. Therefore the TQMxE40M can only be used in COM.0 Revision 2.1 and 3.0 Type10 pinout carrier boards.

3.5.15 CAN interface

The TQMxE40M provides a CAN interface. The signals for the CAN interface are shared with the serial port (SER1) signals and can be configured via a register setting.

If CAN interface is required, appropriate transceivers have to be realized on the carrier.

3.5.16 Watchdog Timer

The TQMxE40M 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 COM Express™ specification does not support external hardware triggering of the watchdog. An external watchdog trigger can be configured to GPIO pins at the COM Express™ connector with the TQ-flexiCFG feature.

3.6 Connectors & LEDs

3.6.1 COM Express™ Connector

A 220-pin receptacle connector with 0.5 mm pitch is used as interface between the TQMxE40M and the carrier board. On the carrier board a 220-pin plug connector with 0.5 mm pitch has to be used.

There are two versions available with 5 mm and 8 mm stacking height.

3.6.2 Debug Header

The TQMxE40M includes a 14-pin flat cable connector, to connect an external debug module (TQ specific), to provide BIOS post code information, debug LEDs and a JTAG interface for on-board FPGA.

This header is intended for TQ internal use only!

Please contact support@tq-group.com for more details about the external debug module.

3.6.3 TQM Debug Card

The TQM debug card is designed to provide access to several processor and chipset control signals.
When the COM Express module is powered up, the uEFI BIOS POST codes are shown.
If the COM Express module does not boot, the uEFI BIOS POST has detected a fatal error and stopped.
The number displayed on the TQM debug card is the number of the test, where the uEFI BIOS boot failed.

Illustration 2: TQM Debug Card

Please contact support@tq-group.com for more details and ordering information about the TQM debug card.

3.6.4 Debug LED

The TQMxE40M includes a dual colour LED providing boot and BIOS information.
The following table shows some LED boot messages.

Table 8: 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 COM Express™ Connector Pinout List

This section describes the TQMxE40M COM Express™ connector pin assignment, which is compliant with COM.0 Revision 3.0 Type10 pinout definitions.

Samples of mating connectors are available from: https://www.ept.de/index.php?tq-colibri-lp

3.7.1 Signal Assignment Abbreviations

Table 9 lists the abbreviations used in Table 10.

Table 9: Abbreviations used in Table 10

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 COM Express™ connector are not used, these signals can be left open on the carrier board, since these signals have a termination on the TQMxE40M.

3.7.2 COM Express™ Connector Pin Assignment

Table 10: COM Express™ Connector Pin Assignment

Pin	Pin-Signal	Description	Type	Remark
A1	GND(FIXED)	Ground	GND	
A2	GBE0_MDI3–	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A3	GBE0_MDI3+	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A4	GBE0_LINK100#	Gigabit Ethernet Controller 0 100 Mbit / sec link indicator	OD	
A5	GBE0_LINK1000#	Gigabit Ethernet Controller 0 1000 Mbit / sec link indicator	OD	
A6	GBE0_MDI2–	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A7	GBE0_MDI2+	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A8	GBE0_LINK#	Gigabit Ethernet Controller 0 link indicator	OD	
A9	GBE0_MDI1–	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A10	GBE0_MDI1+	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A11	GND(FIXED)	Ground	GND	
A12	GBE0_MDI0–	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A13	GBE0_MDI0+	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A14	GBE0_CTREF	Reference voltage for Carrier Board Ethernet channel 0	Power	
A15	SUS_S3#	Indicates system is in Suspend to RAM state low-active output.	O PD	
A16	SATA0_TX+	SATA differential transmit pair 0	O	
A17	SATA0_TX–	SATA differential transmit pair 0	O	
A18	SUS_S4#	Indicates system is in Suspend to Disk state low-active output.	O PD	
A19	SATA0_RX+	SATA differential receive pair 0	I	
A20	SATA0_RX–	SATA differential receive pair 0	I	
A21	GND(FIXED)	Ground	GND	
A22	USB_SSRX0–	SuperSpeed USB3.0 differential receive pair 0	I	
A23	USB_SSRX0+	SuperSpeed USB3.0 differential receive pair 0	I	
A24	SUS_S5#	Indicates system is in Soft Off state low-active output.	O PD	
A25	USB_SSRX1–	SuperSpeed USB3.0 differential receive pair 1	I	
A26	USB_SSRX1+	SuperSpeed USB3.0 differential receive pair 1	I	
A27	BATLOW#	Indicates that external battery is low.	I PU	
A28	(S)ATA_ACT#	SATA activity indicator	O	
A29	AC/HDA_SYNC	Sample-synchronization signal to the CODEC(s)	O	
A30	AC/HDA_RST#	Reset output to CODEC, Active-low	O	
A31	GND(FIXED)	Ground	GND	
A32	AC/HDA_BITCLK	Serial data clock generated by the external CODEC(s)	IO	
A33	AC/HDA_SDOUT	Serial TDM data output to the CODEC	O	
A34	BIOS_DIS0#	Selection straps to determine the BIOS boot device	I PU	
A35	THRMTRIP#	Indicates that the CPU has entered thermal shutdown.	O	
A36	USB6–	USB differential pair 6	IO	
A37	USB6+	USB differential pair 6	IO	
A38	USB_6_7_OC#	USB over-current sense, USB channels 6 and 7	I PU	
A39	USB4–	USB differential pair 4	IO	
A40	USB4+	USB differential pair 4	IO	
A41	GND(FIXED)	Ground	GND	
A42	USB2–	USB differential pair 2	IO	
A43	USB2+	USB differential pair 2	IO	
A44	USB_2_3_OC#	USB over-current sense, USB channels 2 and 3	I PU	
A45	USB0–	USB differential pair 0	IO	
A46	USB0+	USB differential pair 0	IO	
A47	VCC_RTC	Real-time clock circuit-power input. Nominally +3.0 V	Power	
A48	RSVD	Reserved		
A49	GBE0_SDP	Gigabit Ethernet Controller 0 Software-Definable Pin.	IO	TQ-flexiCFG
A50	LPC_SERIRQ/ESPI_CS1#	LPC serial interrupt / eSPI Master Chip Select	IO	
A51	GND(FIXED)	Ground	GND	
A52	RSVD	Reserved		
A53	RSVD	Reserved		
A54	GPI0/SD_DATA0	SDIO Data lines / GPI	IO	TQ-flexiCFG
A55	RSVD	Reserved		

3.7.2 COM Express™ Connector Pin Assignment (continued)

Table 10: COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
A56	RSVD	Reserved		
A57	GND	Ground	GND	
A58	PCIE_TX3+	PCI Express differential transmit pair 3	O	
A59	PCIE_TX3–	PCI Express differential transmit pair 3	O	
A60	GND(FIXED)	Ground	GND	
A61	PCIE_TX2+	PCI Express differential transmit pair 2	O	
A62	PCIE_TX2–	PCI Express differential transmit pair 2	O	
A63	GPI1/SD_DATA1	SDIO Data lines / GPI1	IO	TQ-flexiCFG
A64	PCIE_TX1+	PCI Express differential transmit pair 1	O	
A65	PCIE_TX1–	PCI Express differential transmit pair 1	O	
A66	GND	Ground	GND	
A67	GPI2/SD_DATA2	SDIO Data lines / GPI2	IO	TQ-flexiCFG
A68	PCIE_TX0+	PCI Express differential transmit pair 0	O	
A69	PCIE_TX0–	PCI Express differential transmit pair 0	O	
A70	GND(FIXED)	Ground	GND	
A71	LVDS_A0+/eDP_TX2+	LVDS A or eDP / DP differential pair 2	O	eDP or LVDS
A72	LVDS_A0–/eDP_TX2–	LVDS A or eDP / DP differential pair 2	O	eDP or LVDS
A73	LVDS_A1+/eDP_TX1+	LVDS A or eDP / DP differential pair 1	O	eDP or LVDS
A74	LVDS_A1–/eDP_TX1–	LVDS A or eDP / DP differential pair 1	O	eDP or LVDS
A75	LVDS_A2+/eDP_TX0+	LVDS A or eDP / DP differential pair 0	O	eDP or LVDS
A76	LVDS_A2–/eDP_TX0–	LVDS A or eDP / DP differential pair 0	O	eDP or LVDS
A77	LVDS_VDD_EN	LVDS or eDP panel power enable	O	
A78	LVDS_A3+	LVDS A	O	eDP or LVDS
A79	LVDS_A3–	LVDS A	O	eDP or LVDS
A80	GND(FIXED)	Ground	GND	
A81	LVDS_A_CK+/eDP_TX3+	LVDS A or eDP / DP differential pair 3	O	eDP or LVDS
A82	LVDS_A_CK–/eDP_TX3–	LVDS A or eDP / DP differential pair 3	O	eDP or LVDS
A83	LVDS_I2C_CK/eDP_AUX+	LVDS A I2C_CK or eDP AUX+ signal	IO	eDP or LVDS
A84	LVDS_I2C_DAT/eDP_AUX–	LVDS A I2C_DAT or eDP AUX– signal	IO	eDP or LVDS
A85	GPI3/SD_DATA3	SDIO Data lines / GPI3	IO	TQ-flexiCFG
A86	RSVD	Reserved	I PD	TQ-flexiCFG
A87	eDP_HPD	eDP Detection of Hot Plug	I PD	
A88	PCIE_CLK_REF+	Reference clock output for all PCI Express lanes	O	
A89	PCIE_CLK_REF–	Reference clock output for all PCI Express lanes	O	
A90	GND(FIXED)	Ground	GND	
A91	SPI_POWER	Power supply for Carrier Board SPI	PWR	
A92	SPI_MISO	Data in to TQMxE40M from Carrier Board SPI	I	
A93	GPO0/SD_CLK	SDIO Clock / GPO0	O	TQ-flexiCFG
A94	SPI_CLK	Clock from TQMxE40M to Carrier Board SPI	O	
A95	SPI_MOSI	Data out from TQMxE40M to Carrier Board SPI	O	
A96	TPM_PP	Trusted Platform Module (TPM) Physical Presence pin	I PD	TQ-flexiCFG
A97	TYPE10#	Type10 Module indication (47 kΩ to GND)	O PD	
A98	SER0_TX	Serial port 0 transmitter	O 3V3	without protection
A99	SER0_RX	Serial port 0 receiver	I 3V3	without protection
A100	GND(FIXED)	Ground	GND	
A101	SER1_TX	Serial port 1 transmitter	O 3V3	without protection
A102	SER1_RX	Serial port 1 receiver	I 3V3	without protection
A103	LID#	LID switch	I PU	
A104	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
A105	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
A106	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
A107	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
A108	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
A109	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
A110	GND(FIXED)	Ground	GND	

3.7.2 COM Express™ Connector Pin Assignment (continued)

Table 10: COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
B1	GND(FIXED)	Ground	GND	
B2	GBE0_ACT#	Gigabit Ethernet Controller 0 active indicator	OD	
B3	LPC_FRAME#/ESPI_CS0#	LPC frame indicates the start of an LPC cycle / eSPI	IO	
B4	LPC_AD0/ESPI_IO_0	LPC multiplexed address, command and data bus / eSPI	IO	
B5	LPC_AD1/ESPI_IO_1	LPC multiplexed address, command and data bus / eSPI	IO	
B6	LPC_AD2/ESPI_IO_2	LPC multiplexed address, command and data bus / eSPI	IO	
B7	LPC_AD3/ESPI_IO_3	LPC multiplexed address, command and data bus / eSPI	IO	
B8	LPC_DRQ0#/ESPI_ALERT0#	LPC serial DMA request / eSPI	IO	
B9	LPC_DRQ1#/ESPI_ALERT1#	LPC serial DMA request / eSPI	IO	
B10	LPC_CLK/ESPI_CK	LPC clock output / eSPI	O	
B11	GND(FIXED)	Ground	GND	
B12	PWRBTN#	Power button input	I PU	
B13	SMB_CK	System Management Bus bidirectional clock line	IO	
B14	SMB_DAT	System Management Bus bidirectional data line	IO	
B15	SMB_ALERT#	System Management Bus Alert	I PU	
B16	SATA1_TX+	SATA differential transmit pair 1	O	
B17	SATA1_TX–	SATA differential transmit pair 1	O	
B18	SUS_STAT#/ESPI_RESET	LPC: Indicates imminent suspend operation / eSPI	O	
B19	SATA1_RX+	SATA differential receive pair 1	I	
B20	SATA1_RX–	SATA differential receive pair 1	I	
B21	GND(FIXED)	Ground	GND	
B22	USB_SSTX0–	SuperSpeed USB3.0 differential transmit pair 0	O	
B23	USB_SSTX0+	SuperSpeed USB3.0 differential transmit pair 0	O	
B24	PWR_OK	Power OK from main power supply	I PU	
B25	USB_SSTX1–	SuperSpeed USB3.0 differential transmit pair 1	O	
B26	USB_SSTX1+	SuperSpeed USB3.0 differential transmit pair 1	O	
B27	WDT	Watchdog time-out	O	TQ-flexiCFG
B28	AC/HDA_SDIN2	Serial TDM data input	I	N/A
B29	AC/HDA_SDIN1	Serial TDM data input	I PU	
B30	AC/HDA_SDIN0	Serial TDM data input	I PU	
B31	GND(FIXED)	Ground	GND	
B32	SPKR	PC Audio Speaker output	O	
B33	I2C_CK	General purpose I^2C port clock output	IO	
B34	I2C_DAT	General purpose I^2C port data I/O line	IO	
B35	THRM#	Input from Carrier Board temperature sensor	I PU	
B36	USB7–	USB differential pair 7	IO	
B37	USB7+	USB differential pair 7	IO	
B38	USB_4_5_OC#	USB over-current sense, USB channels 4 and 5	I PU	
B39	USB5–	USB differential pair 5	IO	
B40	USB5+	USB differential pair 5	IO	
B41	GND(FIXED)	Ground	GND	
B42	USB3–	USB differential pair 3	IO	
B43	USB3+	USB differential pair 3	IO	
B44	USB_0_1_OC#	USB over-current sense, USB channels 0 and 1	I PU	
B45	USB1–	USB differential pair 1	IO	
B46	USB1+	USB differential pair 1	IO	
B47	ESPI_EN#	The Carrier shall tie ESPI_EN# to GND for eSPI operation, LPC NC	I PU	TQ-flexiCFG
B48	USB0_HOST_PRSNT	Module USB client may detect the presence of a USB host on USB0	I PD	TQ-flexiCFG
B49	SYS_RESET#	Reset button input	I PU	
B50	CB_RESET#	Reset output from TQMxE40M to carrier board	O	
B51	GND(FIXED)	Ground	GND	
B52	RSVD	Reserved		
B53	RSVD	Reserved		
B54	GPO1/SD_CMD	SDIO Command / GPO1	O	TQ-flexiCFG
B55	RSVD	Reserved		

3.7.2 COM Express™ Connector Pin Assignment (continued)

Table 10: COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
B56	RSVD	Reserved		
B57	GPO2 / SD_WP	SDIO Write Protect / GPO2	O	TQ-flexiCFG
B58	PCIE_RX3+	PCI Express differential receive pair 3	I	
B59	PCIE_RX3–	PCI Express differential receive pair 3	I	
B60	GND(FIXED)	Ground	GND	
B61	PCIE_RX2+	PCI Express differential receive pair 2	I	
B62	PCIE_RX2–	PCI Express differential receive pair 2	I	
B63	GPO3/SD_CD#	SDIO Card Detect / GPO3	O	TQ-flexiCFG
B64	PCIE_RX1+	PCI Express differential receive pair 1	I	
B65	PCIE_RX1–	PCI Express differential receive pair 1	I	
B66	WAKE0#	PCI Express wake up signal	I PU	
B67	WAKE1#	General purpose wake up signal	I PU	
B68	PCIE_RX0+	PCI Express differential receive pair 0	I	
B69	PCIE_RX0–	PCI Express differential receive pair 0	i	
B70	GND(FIXED)	Ground	GND	
B71	DDI0_PAIR0+	DDI0 DP / HDMI / DVI differential pair 0	O	
B72	DDI0_PAIR0–	DDI0 DP / HDMI / DVI differential pair 0	O	
B73	DDI0_PAIR1+	DDI0 DP / HDMI / DVI differential pair 1	O	
B74	DDI0_PAIR1–	DDI0 DP / HDMI / DVI differential pair 1	O	
B75	DDI0_PAIR2+	DDI0 DP / HDMI / DVI differential pair 2	O	
B76	DDI0_PAIR2–	DDI0 DP / HDMI / DVI differential pair 2	O	
B77	(DDI0_PAIR4+) SER0_RTS#	Serial port 0 Request To Send	O	TQ-flexiCFG
B78	(DDI0_PAIR4–) SER0_CTS#	Serial port 0 Clear To Send	I PU	TQ-flexiCFG
B79	LVDS_BKLT_EN	LVDS or eDP panel backlight enable	O	
B80	GND(FIXED)	Ground	GND	
B81	DDI0_PAIR3+	DDI0 DP / HDMI / DVI differential pair 3	O	
B82	DDI0_PAIR3–	DDI0 DP / HDMI / DVI differential pair 3	O	
B83	LVDS_BKLT_CTRL	LVDS or eDP panel backlight brightness control	O	
B84	VCC_5V_SBY	Standby power input: +5.0 V nominal	PWR	
B85	VCC_5V_SBY	Standby power input: +5.0 V nominal	PWR	
B86	VCC_5V_SBY	Standby power input: +5.0 V nominal	PWR	
B87	VCC_5V_SBY	Standby power input: +5.0 V nominal	PWR	
B88	BIOS_DIS1#	Selection straps to determine the BIOS boot device	I PU	
B89	DDI0_HPD	DDI0 Detection of Hot Plug	I PD	
B90	GND(FIXED)	Ground	GND	
B91	(DDI0_PAIR5+) SER1_RTS#	Serial port 1 Request To Send	O	
B92	(DDI0_PAIR5–) SER1_CTS#	Serial port 1 Clear To Send	I PU	
B93	DDI0_PAIR6+	DDI0 differential pair 6	O	N/A
B94	DDI0_PAIR6–	DDI0 differential pair 6	O	N/A
B95	DDI0_DDC_AUX_SEL	Selects the function of DDI0_CTRLxAUX+/– Signals	I PD	
B96	USB7_HOST_PRSNT	Module USB client may detect the presence of a USB host on USB7	I PD	TQ-flexiCFG
B97	SPI_CS#	Chip select for Carrier Board SPI	O	
B98	DDI0_CTRLCLK_AUX+	DDI0_CTRLCLK_AUX+ signal DP AUX, HDMI / DVI CLK	IO	
B99	DDI0_CTRLDATA_AUX–	DDI0_CTRLDATA_AUX– signal DP AUX, HDMI / DVI DATA	IO	
B100	GND(FIXED)	Ground	GND	
B101	FAN_PWMOUT	Fan Pulse Width Modulation speed control output	O	TQ-flexiCFG
B102	FAN_TACHIN	Fan tachometer input	I PU	
B103	SLEEP#	Sleep button	I PU	
B104	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
B105	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
B106	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
B107	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
B108	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
B109	VCC_12V	Primary wide power input 4.75 V – 20 V	PWR	
B110	GND(FIXED)	Ground		

4. MECHANICS

4.1 TQMxE40M Dimensions

The dimensions of the TQMxE40M are 84 mm × 55 mm (±0.2 mm).
The following illustration shows the three-sided drawing of the TQMxE40M:

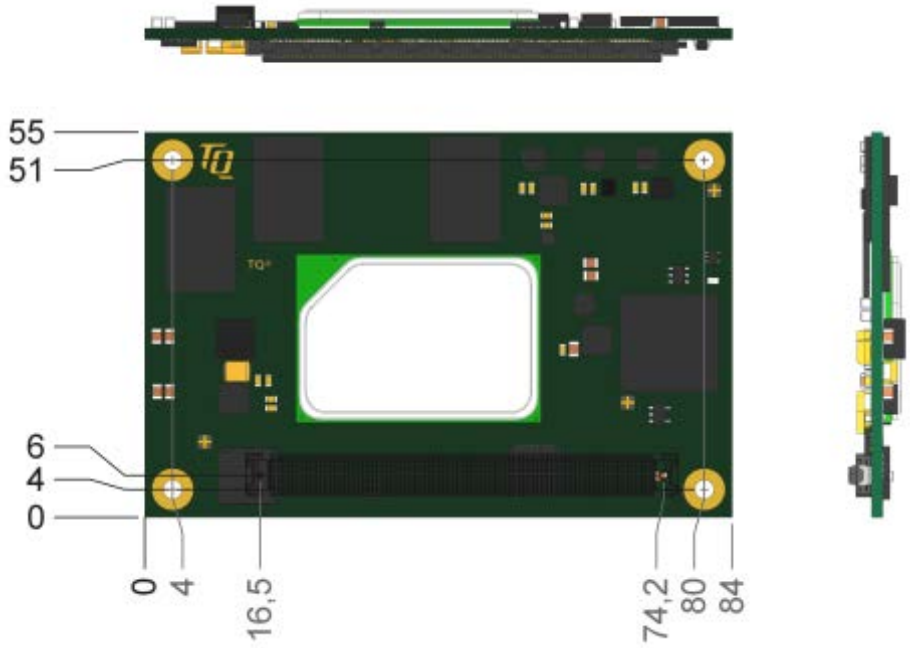


Illustration 3: Three-sided drawing of the TQMxE40M (dimensions in mm)

The following illustration shows the bottom view of the TQMxE40M:

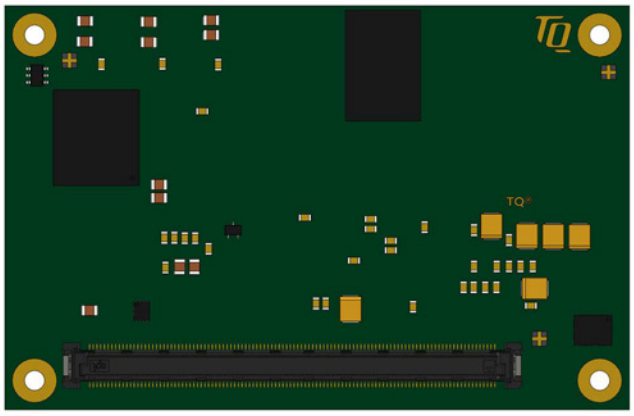


Illustration 4: Bottom view drawing of the TQMxE40M

4.2 Heat Spreader

Two different heat spreaders are available for the TQMxE40M:

- Standard: TQMxE40M-HSP-AB (11 mm): Heat spreader for TQMxE40M according to the COM Express™ specification (13 mm ±0.2 mm, including PCB).
- Low-Profile: TQMxE40M-HSP-AA (6 mm): Heat spreader for TQMxE40M, low profile for designs with very low heights (8 mm ±0.2 mm including PCB).

The following illustration shows the standard heat spreader for the TQMxE40M.

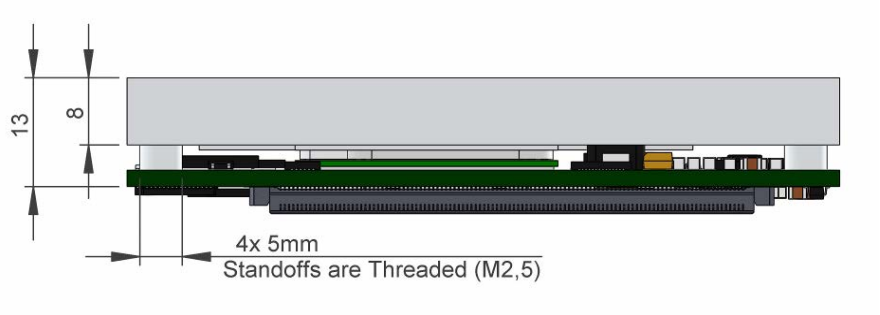


Illustration 5: Standard Heat Spreader

The following illustration shows the low profile heat spreader for the TQMxE40M.

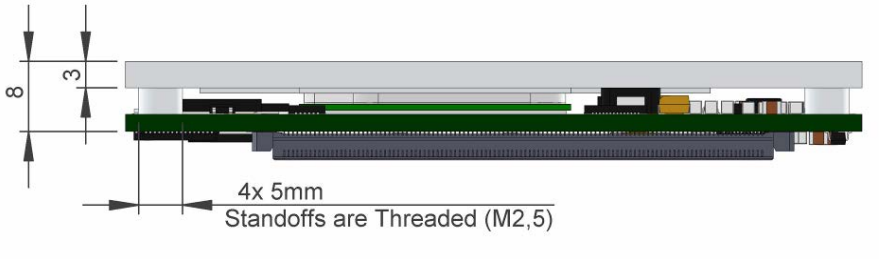


Illustration 6: Low-Profile Heat Spreader

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.
The White Paper “Heat Spreader Mounting Instruction” provides information how to mount the heat spreader.
Please contact support@tq-group.com for more details about 2D/3D Step models.

4.3 Mechanical and Thermal Considerations

The TQMxE40M 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 TQMxE40M. 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 use passive or active cooling, the thermal interface to the heat spreader is always the same.

Attention: Thermal Considerations	
	Do not operate the TQMxE40M 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 TQMxE40M 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.

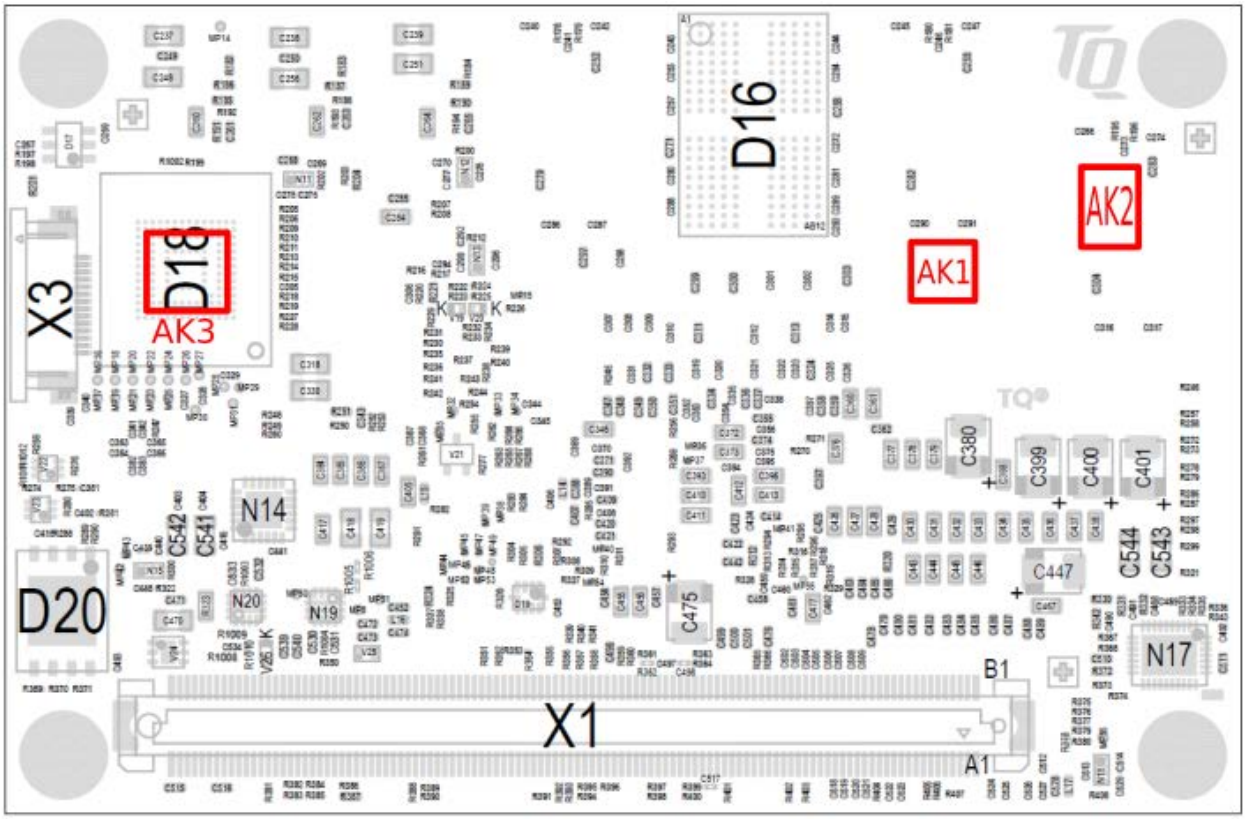
Please contact support@tq-group.com for further details.

4.5 Label placement

Table 11: Labels on TQMxE40M

Label	Content
AK1	MAC address
AK2	TQMxE40M version and revision
AK3	License label

Illustration 7: Label Placement



5. Software

5.1 System Resources

5.1.1 I²C Bus

The TQMxE40M 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 COM Express™ I²C port.

Table 12: I²C address mapping COM Express™ I²C port

8-bit Address	Function	Remark
0xA0	TQMxE40M EEPROM	–
0xAE	Carrier Board EEPROM	Embedded EEPROM configuration not supported

5.1.2 SMBus

The TQMxE40M provides a System Management Bus (SMBus). There are no SMBus devices on the TQMxE40M.

5.1.3 Memory Map

The TQMxE40M 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 TQMxE40M 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 TQMxE40M supports various operating systems:

- Microsoft® Windows® 10 (LTSC 2019)
- 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 TQMxE40M 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 TQMxE40M 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 COM Express™ 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 TQMxE40M 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>.

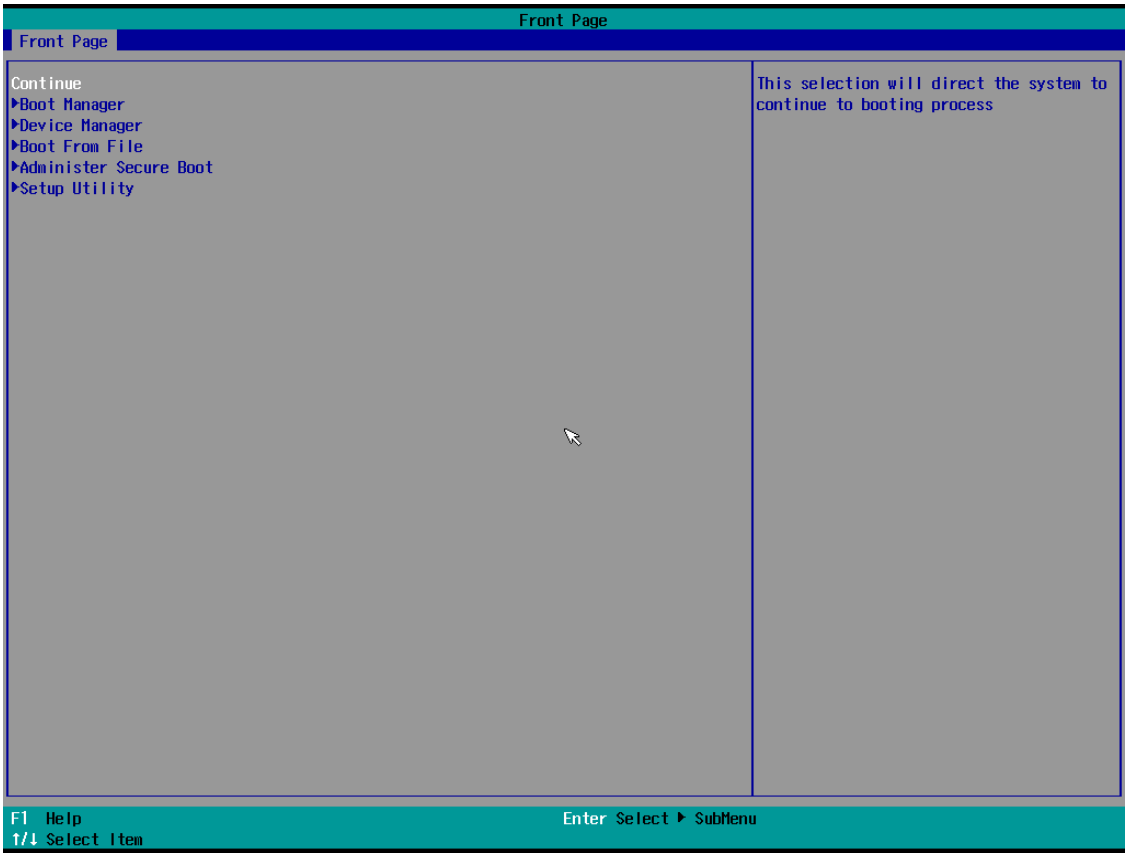


Illustration 8: InsydeH2O BIOS Front Page

6.1 Continue Boot Process

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

6.4 Boot from File

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

6.5 Administer Secure Boot

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

Note: Secure Boot	
	This option should only be used by advanced users.

6.6 Setup Utility

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

Key:

↑ / ↓	Navigate between setup items.
← / →	Navigate between setup screens (Main, Advanced, Security, Power, Boot and Exit).
<F1>	Show general help screen (Key Legend).
<F5> / <F6>	In the main screen this buttons allow to change between different languages. Otherwise it allows to change the value of highlighted menu item.
<ENTER>	Press to display or change setup option listed for a certain menu or to display setup sub-screens.
<F9>	Press to load the setup default configuration of the board which cannot be changed by the user. This option has to be confirmed and saved by <F10> afterwards. Leaving the InsydeH2O Setup Utility will discard the changes.
<F10>	Press to save any changes made and exit setup utility by executing a restart.
<ESC>	Press to leave the current screen or sub-screen and discard all changes.

6.6.1 Main

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

Menu Item	Option	Description
Platform Information	See submenu	Shows some platform information.
Language	English / French / Korean / Chinese	Configures the language of the InsydeH2O Setup Utility
System Time	HH:MM:SS	Use to change the system time to the 24-hour format
System Date	MM:DD:YYYY	Use to change the system date
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 disables BIOS ACPI auto configuration
Enable Hibernation	[ ] / [X]	Enables or disables system ability to hibernate (OS/S4 Sleep State). This option may not be effective with some OSs.
PTID Support	[ ] / [X]	PTID support will be loaded if enabled.
PECI Access Method	Direct I/O / ACPI	PECI access method is Direct I/O or ACPI.
ACPI S3 support	Enabled / Disabled	Enable ACPI S3 support.
Native PCIE Enable	Enabled / Disabled	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 ACPI Lower Power S0 Idle Capability is enabled (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.
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.

Menu Item	Option	Description
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.
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 bi 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_ADDRBASE+offset to MWAIT(offste). 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_POWR_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 1/8 W when programming. 0 = no custom override. For 12.50 W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP Limit. If value is 0, BIOS 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 1/8 W when programming. If the value is 0, BIOS will program this value as 1.25*TDP. For 12.5 W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
1-Core Ratio Limit Override	[X]	Note: Option only shown when Power Limit 2 enabled. 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 (RP0). Value beyond the range will be clipped to min/max supported by SKU.
Disable Turbo GT frequency	Enabled / Disabled	Enabled: Disables Turbo GT frequency Disabled: GT frequency is not limited

6.6.2.5.4 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.
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 3rd 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 0th is enabled, 0th will become visible.
PCIe EQ settings	See submenu	This form contains options for controlling PCIe EQ process.
PCI Express Root Port X	See submenu	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 transmitter preset	0 – 10	Choose the value of the preset that will be used during phase 1 of the 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.

Menu Item	Options	Description
EDPC	Enabled / Disabled	Enable or Disable Rootport extensions for Downstream Port Containment.
URR	Enabled / Disabled	PCI Express Unsupported Request Reporting enable/disable.
FER	Enabled / Disabled	PCI Express Device Fatal Error Reporting enable/disable.
NFER	Enabled / Disabled	PCI Express Device Non-Fatal Error Reporting enable/disable.
CER	Enabled / Disabled	PCI Express Device Correctable Error Reporting enable/disable.
SEFE	Enabled / Disabled	Root PCI Express System Error on Fatal Error enable/disable.
SENFE	Enabled / Disabled	Root PCI Express System Error on Non-Fatal Error enable/disable.
SECE	Enabled / Disabled	Root PCI Express System Error on Correctable Error enable/disable.
PME SCI	Enabled / Disabled	PCI Express PME SCI enable/disable.
Hot Plug	Enabled / Disabled	PCI Express Hot Plug enable/disable.
Advanced Error Reporting	Enabled / Disabled	Advanced Error Reporting enable/disable.
PCIe Speed	Auto / Gen1 / Gen2 / Gen3	Configure PCIe Speed.
Transmitter Half Swing	Enabled / Disabled	Transmitter Half Swing enable/disable.
Detect Timeout	[X]	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
Extra Bus Reserved	[X]	Extra Bus Reserved (0-7) for bridges behind this Root Bridge.
Reserved Memory	[X]	Reserved Memory for this Root Bridge (1-20) MB.
Reserved 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. 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.

Menu Item	Options	Description
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. Note: This option is only configurable if "DITO Configuration" is enabled.
DM Value	0 – 15	DM Value. Note: 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 onlay – 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) Note: Ensure CAN is also enabled in SioTqmx86 'COM Express Serial Port 1 Routing'
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) Note: Ensure CAN is also enabled in SioTqmx86 'COM Express Serial Port 1 Routing'

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.

Menu Item	Options	Description
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.

Menu Item	Option	Description
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 / Ultra Low Power	Configure Power State S5. Normal: Wakeup over LAN (WOL), timer, external Wake and Power Button possible. Ultra Low Power: Wakeup over 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)!
GPIO/SD-Card configuration	GPIO interface SD-Card interface	Configure the COM Express configuration as GPIO or SD-Card interface

Menu Item	Option	Description
Display Port B Aux Selection	DDC/AUX selection over RSVD9 pin (AUX is HW default) / DDC I2C is enabled	Choose if DDC I2C is enabled for DP_B or DDC/AUX selected over RSVD9 pin (A86). Note: For DDC/AUX selection AUX is HW default.
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).
COM Express Serial Port 1 Routing	CPLD UART 1 / CAN 1	Configure Multiplexer of Serial Port 1 either to CPLD UART 1 or CAN 1. Note: Ensure CAN is also enabled in 'PSE Configuration'!
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 Samsung LTM230 HT / 1366 × 768 @ 60 Hz NXP Generic / 320 × 240 @ 60 Hz NXP Generic	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.

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 /	Console Redirection text mode resolution. Auto: Follow VGA text mode

Menu Item	Option	Description
	Force 80x24 (DEL FIRST ROW) / Force 80x24 (DEL LAST ROW)	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 / HSUART 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.

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.

Menu Item	Option	Description
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.
EFI / Legacy	Submenu depends on bootable devices	Option to adapt boot order. Selection depends on boot devices connected. Note: Add Boot Options has to be configured as First or Last. The order can be changed by pressing <F5> or <F6>.

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 TQMxE40M.
Please read the entire instructions before beginning the BIOS update.
By disregarding the information you can destroy the uEFI BIOS on the TQMxE40M!
This document will guide the customer to update the uEFI BIOS on the TQMxE40M by using the Insyde Flash Firmware Tools.
Please contact support@tq-group.com for more information to the latest uEFI BIOS version for the TQMxE40M.

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)
  - Be sure to have H2OFFT Version 200.00.00.13 or later
- 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.

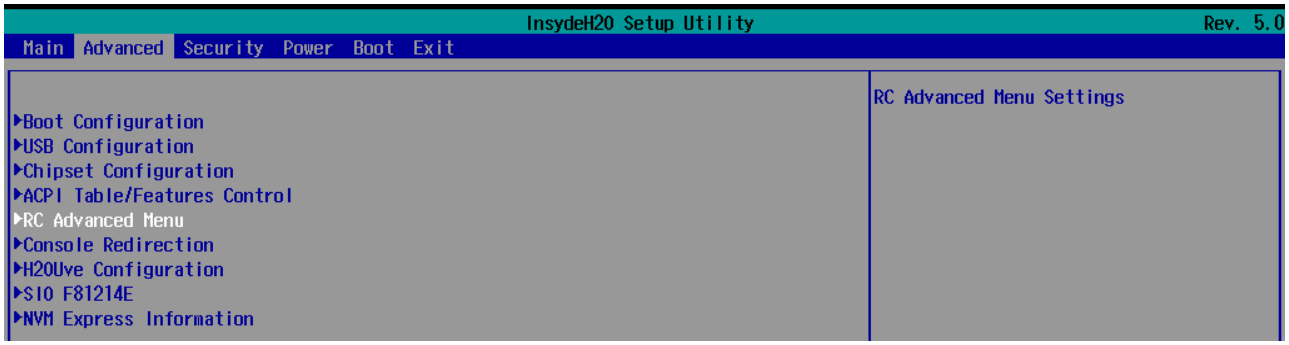


Illustration 9: RC Advanced Menu

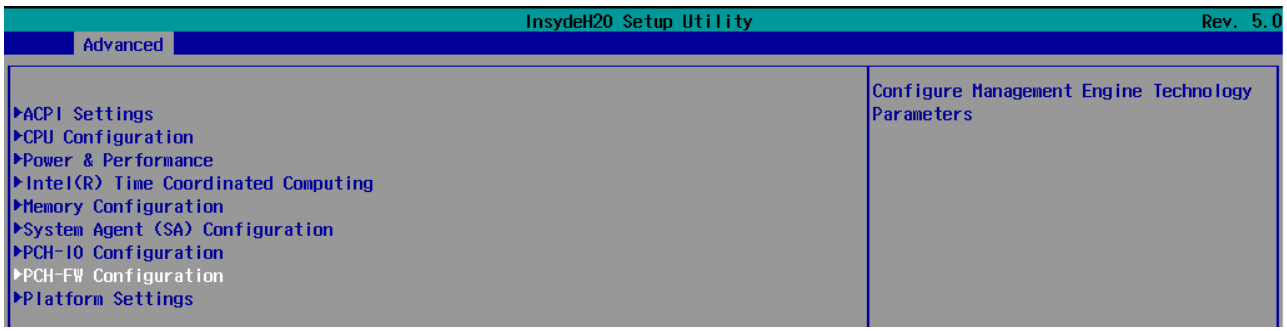


Illustration 10: PCH-FW Configuration menu

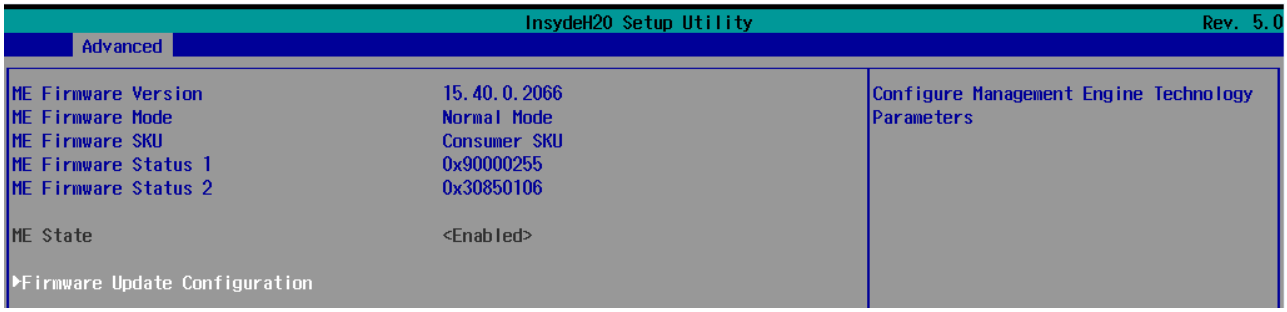


Illustration 11: Firmware Update Configuration menu

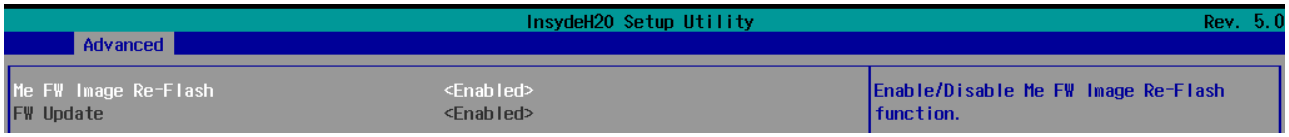


Illustration 12: ME FW Image Re-Flash option

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".

Illustration 13: 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.

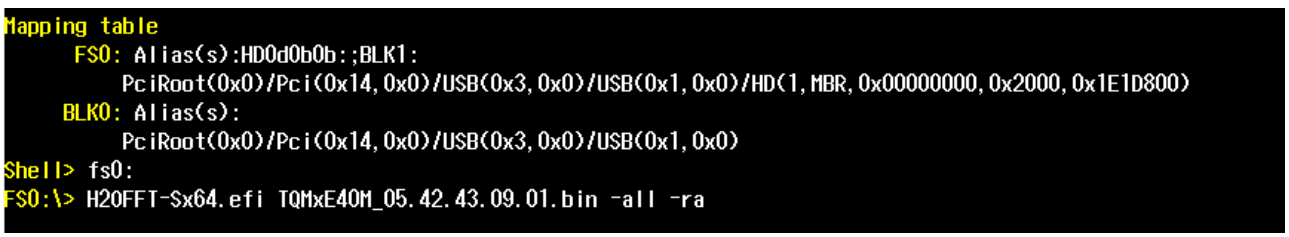


Illustration 14: EFI Shell uEFI BIOS Update

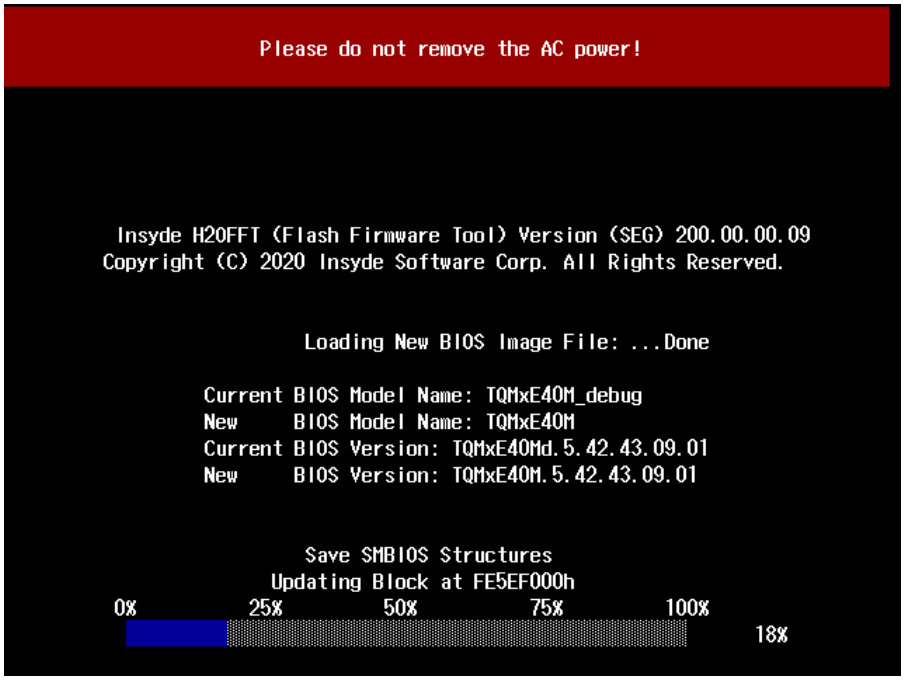


Illustration 15: Screen during BIOS Update

6.7.4 Step 3b: Updating uEFI BIOS via Windows Operating System

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

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

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

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

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

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

6.7.5 Step 4: BIOS update check on the TQMxE40M Module

After the uEFI BIOS update, the new uEFI BIOS configures the complete TQMxE40M hardware and this results in some reboots and the first boot time takes longer (up to 1 minute).

The TQMxE40M includes a dual colour Debug LED providing boot and uEFI BIOS information.

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

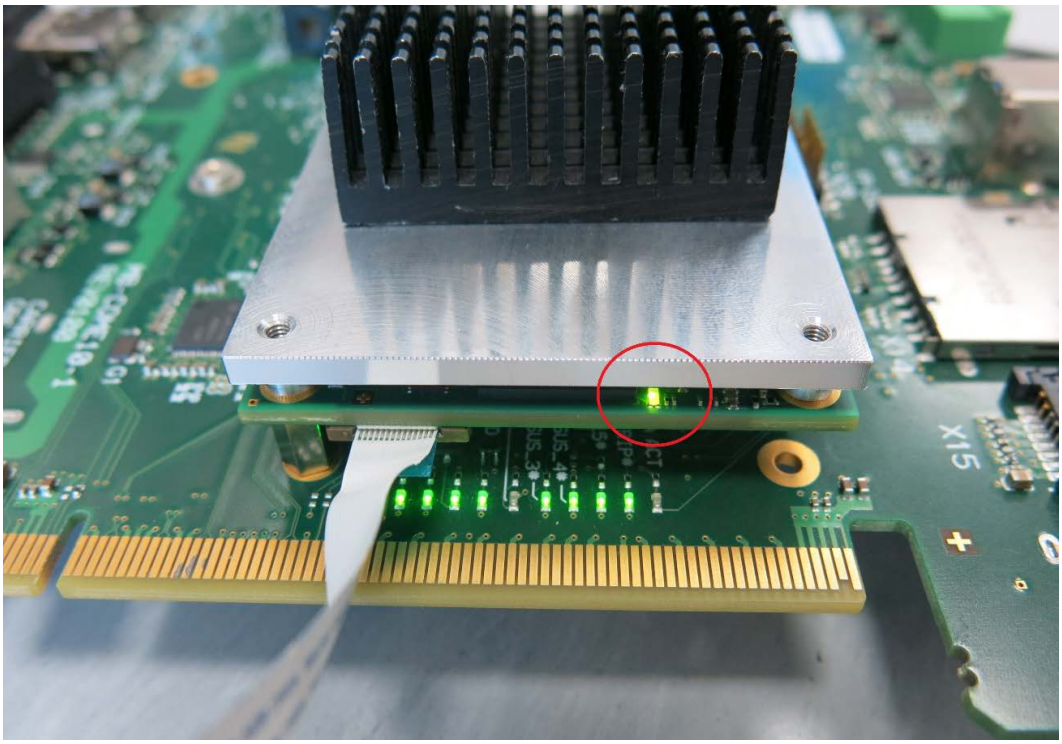


Illustration 16: TQMxE40M Debug LED

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.

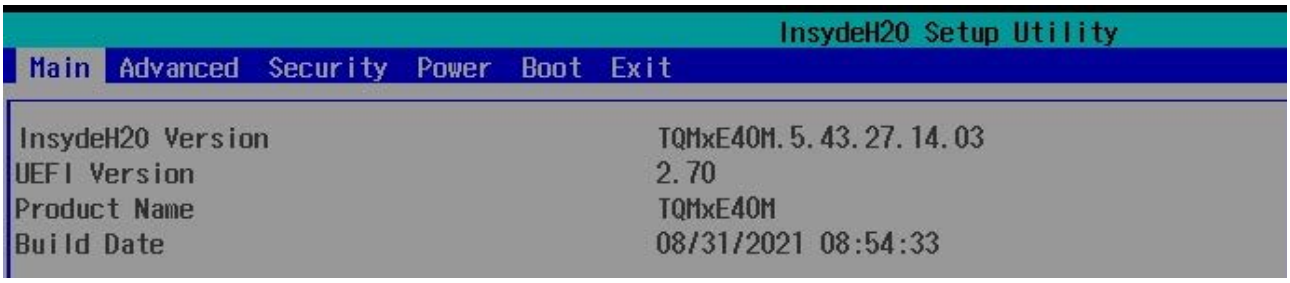


Illustration 17: EFI BIOS Main Menu

7. SAFETY REQUIREMENTS AND PROTECTIVE REGULATIONS

7.1 EMC

The TQMxE40M 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 interspersion on the signal path from the input to the protection circuit in the system, the protection against electrostatic discharge should be arranged directly at the inputs of a system. As these measures always have to be implemented on the carrier board, no special preventive measures were done on the TQMxE40M.

7.3 Shock & Vibration

The TQMxE40M 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 Cyber Security

A Threat Analysis and Risk Assessment (TARA) must always be performed by the customer for their individual end application, as the TQMxE40M is only a sub-component of an overall system.

7.6 Export Control and Sanctions Compliance

The customer is responsible for ensuring that the product purchased from TQ is not subject to any national or international export/import restrictions. If any part of the purchased product or the product itself is subject to said restrictions, the customer must procure the required export/import licenses at its own expense. In the case of breaches of export or import limitations, the customer indemnifies TQ against all liability and accountability in the external relationship,irrespective of the legal grounds. If there is a transgression or violation, the customer will also be held accountable for any losses, damages or fines sustained by TQ. TQ is not liable for any delivery delays due to national or international export restrictions or for the inability to make a delivery as a result of those restrictions. Any compensation or damages will not be provided by TQ in such instances.

The classification according to the European Foreign Trade Regulations (export list number of Reg. No. 2021/821 for dual-use-goods) as well as the classification according to the U.S. Export Administration Regulations in case of US products (ECCN according to the U.S. Commerce Control List) are stated on TQ´s invoices or can be requested at any time. Also listed is the Commodity code (HS) in accordance with the current commodity classification for foreign trade statistics as well as the country of origin of the goods requested/ordered.

7.7 Warranty

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

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

7.8 Reliability and service life

The MTBF according to MIL-HDBK-217F N2 is 417 858 hours, Ground Benign, at +40 °C.

8. ENVIRONMENT PROTECTION

8.1 RoHS

The TQMxE40M is manufactured RoHS compliant.

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

8.2 WEEE®

The final distributor is responsible for compliance with the WEEE® regulation.

Within the scope of the technical possibilities, the TQMxE40M was designed to be recyclable and easy to repair.

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 Statement on California Proposition 65

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

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

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

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

8.5 EuP

The Eco Design Directive, also Energy using Products (EuP), is applicable to products for the end user with an annual quantity >200,000. The TQMxE40M must therefore always be seen in conjunction with the complete device. The available standby and sleep modes of the components on the TQMxE40M enable compliance with EuP requirements for the TQMxE40M.

8.6 Battery

No batteries are assembled on the TQMxE40M.

8.7 Packaging

By environmentally friendly processes, production equipment and products, we contribute to the protection of our environment. To be able to reuse the TQMxE40M, 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 TQMxE40M is delivered in reusable packaging.

8.8 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 13: 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
ECC	Error-Correting Code
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
HDA	High Definition Audio
HDMI	High Definition Multimedia Interface
HEVC	High Efficiency Video Coding
HFM	High Frequency Mode
HPD	Hot Plug Detection
IBECC	In Band ECC (Error-Correting Code)
I/O	Input Output
I^2C	Inter-Integrated Circuit
IDE	Integrated Device Electronics
IEEE®	Institute of Electrical and Electronics Engineers
IO	Input Output
IoT	Internet of Things
IP	Ingress Protection
IRQ	Interrupt Request
JEIDA	Japan Electronic Industries Development Association
JPEG	Joint Photographic Experts Group
JTAG®	Joint Test Action Group
LED	Light Emitting Diode

9.1 Acronyms and definitions (continued)

Table 13: Acronyms (continued)

Acronym	Meaning
LP	Low Power or Low Profile
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
SIMD	Single Instruction Multiple Data
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 14: Further applicable documents and links

No.	Name	Rev., Date	Company
(1)	PICMG® COM Express™ Module Base Specification	Rev. 3.0, March 31, 2017	PICMG®
(2)	PICMG® COM Express™ Carrier Design Guide	Rev. 2.0, Dec. 6, 2013	PICMG®
(3)	PICMG® COM Express™ Embedded Application Programming Interface	Rev. 1.0, Aug. 8, 2010	PICMG®

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

Technology in Quality