TQMx110EB
User's Manual

TQMx110EB UM 0100
11.03.2022

TABLE OF CONTENTS

TABLE DIRECTORY

FIGURE DIRECTORY

REVISION HISTORY

Rev.	Date	Name	Pos.	Modification
0100	11.03.2022	KG		First release

1. ABOUT THIS MANUAL

1.1 Copyright and License Expenses

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

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

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

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

1.2 Registered Trademarks

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

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

1.3 Disclaimer

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

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

1.4 Imprint

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

Tel: +49 8153 9308–0
Fax: +49 8153 9308–4223
E-Mail: Info@TQ-Group
Web: TQ-Group

1.5 Service and Support

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

You can register on our website www.tq-group.com to have access to restricted information and automatic update services.

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

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

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

1.6 Tips on Safety

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

1.7 Symbols and Typographic Conventions

Table 1: Terms and Conventions

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

1.8 Handling and ESD Tips

General handling of your TQ-products

	The TQ-product may only be used and serviced by certified personnel who have taken note of the information, the safety regulations in this document and all related rules and regulations. A general rule is: do not touch the TQ-product during operation. This is especially important when switching on, changing jumper settings or connecting other devices without ensuring beforehand that the power supply of the system has been switched off. Violation of this guideline may result in damage / destruction of the TQMx110EB and be dangerous to your health. Improper handling of your TQ-product would render the guarantee invalid.

Proper ESD handling

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

1.9 Naming of Signals

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

Example: RESET#

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

Example: C / D#

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

The identification of the individual functions follows the above conventions.

Example: WE2# / OE#

1.10 Further Applicable Documents / Presumed Knowledge

- **Specifications and manual of the modules used:**
  These documents describe the service, functionality and special characteristics of the module used.
- **Specifications of the components used:**
  The manufacturer's specifications of the components used, for example CompactFlash cards, are to be taken note of. They contain, if applicable, additional information that has to be taken note of for safe and reliable operation. These documents are stored at TQ-Systems GmbH.
- **Chip errata:**
  It is the user's responsibility to make sure all errata published by the manufacturer of each component are taken note of. The manufacturer's advice should be 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 (3), 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 (2), (4).

2. INTRODUCTION

Based on the internationally established PICMG® standard COM Express™ (COM.0 R3.0), the TQMx110EB enables the design of not only powerful but also economical x86 based systems. The user has access to all essential interfaces of the CPU at the Type 6 compliant pin out connector. Hence all features of the 11th Generation Intel® Core™ and XEON® H can be used. The direct access to all interfaces gives the user the freedom to use the features of the CPU in the most suitable way for his application.

The compact and robust design as well as the option of conformal coating extends the use cases to applications within rugged industry, transportation and aviation environments. Based on the very low-power consumption and the extended temperature support it is also possible to realize outdoor applications in an easy and reliable way.

2.1 Overview

The following key functions are implemented on the TQMx110EB:

Processor:

11th Generation Intel® Core™ embedded series (TigerLake-H) with up to 8 processor cores

- Intel® Core™ i7-11850HE 8 × 2.6 GHz / 4.7 GHz Turbo, 24 MB Cache, 45 W (cTDP 35 W), 0 °C – 100 °C
- Intel® Core™ i5-11500HE 6 × 2.6 GHz / 4.5 GHz Turbo, 12 MB Cache, 45 W (cTDP 35 W), 0 °C – 100 °C
- Intel® Core™ i3-11100HE 4 × 2.4 GHz / 4.4 GHz Turbo, 8 MB Cache, 45 W (cTDP 35 W), 0 °C – 100 °C

11th Generation Intel® XEON® H embedded / industrial series (TigerLake-H) with up to 8 processor cores

- Intel® XEON® W-11865MRE 8 × 2.6 GHz / 4.7 GHz Turbo, 24 MB Cache, 45 W (cTDP 35 W), -40 °C – 100 °C
- Intel® XEON® W-11555MRE 6 × 2.6 GHz / 4.5 GHz Turbo, 12 MB Cache, 45 W (cTDP 35 W), -40 °C – 100 °C
- Intel® XEON® W-11155MRE 4 × 2.4 GHz / 4.4 GHz Turbo, 8 MB Cache, 45 W (cTDP 35 W), -40 °C – 100 °C

11th Generation Intel® XEON® H low power embedded / industrial series (TigerLake-H) with up to 8 processor cores

- Intel® XEON® W-11865MLE 8 × 1.5 GHz / 4.5 GHz Turbo, 24 MB Cache, 25 W, 0 °C – 100 °C
- Intel® XEON® W-11555MLE 6 × 1.9 GHz / 4.4 GHz Turbo, 12 MB Cache, 25 W, 0 °C – 100 °C
- Intel® XEON® W-11155MLE 4 × 1.8 GHz / 3.1 GHz Turbo, 8 MB Cache, 25 W, 0 °C – 100 °C

Memory:

- 2 × DDR4 SO-DIMM socket with max. 64 Gbyte, dual channel DDR4 up to 3200 MT/s SO-DIMM modules (optionally with ECC support, only on Intel® XEON® H CPU type)
- M.2 BGA SSD with PCIe Gen 3 x4 up to 1 Tbyte
- Support of Intel® Optane™ memory technology via PCIe
- EEPROM: 32 kbit (24AA32) (optional)

Graphics:

- 3 × Digital Display Interface / DP++ with up to 8K; DisplayPort 1.4a with support for Multi-Stream Transport (MST)
- 1 × Embedded Digital Display Interface (eDP) or dual channel LVDS interface (eDP 1.4b or dual LVDS)

Peripheral interfaces:

- 1 × 2.5 Gigabit Ethernet (Intel® i225)
- 4 × USB 3.2 Gen 2 (up to 10 Gb/s) with USB 3.0 compatibility
- 8 × USB 2.0
- 4 × SATA Gen 3 (up to 6 Gb/s) or 4x PCIe Gen 3 (up to 8 Gb/s)
- 8 × PCIe Gen 3 (up to 8 Gb/s) (8 (×1), 4 (×2), or 2 (×4))
- 1 × PCIe PEG port Gen 4 (up to 16 Gb/s) (1 (×16), 2 (×8), or 2 (×4) + 1 (×8))
- 1 × LPC or eSPI bus
- 1 × Intel® HD audio (HDA)
- 1 × I^2C (2^{nd} I^2C optional) (master/slave capable)
- 1 × SMBus
- 1 × SPI (for external uEFI BIOS flash)
- 2 × Serial port (Rx/Tx, legacy compatible), 4-wire (Rx/Tx/RTS/CTS) optionally through TQ-flexiCFG
- 8 × GPIO through TQ-flexiCFG

Security components:

- TPM discrete SLB9670 TPM 2.0 controller or internal firmware TPM (FTPM)

Others:

- TQMx86 board controller with Watchdog and TQ-flexiCFG
- Hardware monitor

Power supply voltage:

- Nominal voltage 12 V (11.4 V to 12.6 V)
- 5 V Standby (optional) 5 V (4.75 V to 5.25 V)
- 3 V Battery for RTC

Environment:

- Operating Standard temperature: 0 °C to +60 °C
- Operating Extended temperature: –40 °C to +75 °C
- Storage temperature: –40 °C to +85 °C
- Relative humidity (operation): 10 % to 90 % (non-condensing)
- Relative humidity (storage): 5 % to 95 % (non-condensing, with conformal coating)

Form factor / dimensions:

- COMExpress™ Basic, Type 6, 125 × 95 mm²

2.2 Compliance

The TQMx110EB complies with PICMG® COM Express™ Module Base Specification (COM.0 R3.0).

2.3 Versions

The TQMx110EB is available in several standard configurations

Table 2: TQMx110EB 11th Generation Intel® Core™ Embedded Series configurations and features

Feature	TQMx110EB-AA	TQMx110EB-AB	TQMx110EB-AC
CPU	8-core	6-core	4- Core
Intel	Core™ i7-11850HE	Core™ i5-11500HE	Core™ i3-11500HE
CPU TDP	45 / 35 W	45 / 35 W	45 / 35 W
CPU Clock (Base)	2.4 GHz	2.6 GHz	2.4 GHz
L2 Cache	24 MB	12 MB	8 MB
Heat spreader	TQMx110EB-HSP-AA	TQMx110EB-HSP-AA	TQMx110EB-HSP-AA
Heatsink incl. fan	TQMx110EB-KK-AA	TQMx110EB-KK-AA	TQMx110EB-KK-AA
DRAM / SO-DIMM	16 / 32 / 64 GB	16 / 32 / 64 GB	16 / 32 / 64 GB
DRAM / ECC	no	no	no
Use Condition	Embedded	Embedded	Embedded
Operating Temperature	0 °C to +60 °C (Turbo ON) 0 °C to +75 °C (35 W Turbo OFF)	0 °C to +60 °C (Turbo ON) 0 °C to +75 °C (35 W Turbo OFF)	0 °C to +60 °C (Turbo ON) 0 °C to +75 °C (35 W Turbo OFF)
M.2 BGA SSD PCIe x4	--	--	--
TPM 2.0	1	1	1
Independent displays	4	4	4
LVDS or eDP	1	1	1
DP or HDMI	3	3	3
2.5 GbE	1	1	1
USB 2.0 host	8	8	8
USB 3.2 host	4	4	4
SATA Gen 3	4	4	4
PCIe Gen 3 ×1	8	8	8
PEG Gen 4 x16	1	1	1
I2C / SPI	1 / 1	1 / 1	1 / 1
HDA	1	1	1
LPC or eSPI	1	1	1
UART / GPIO	2 / 8	2 / 8	2 / 8

Table 3: TQMx110EB 11th Generation Intel® XEON® H Embedded Series configurations and features

Feature	TQMx110EB-AD	TQMx110EB-AE	TQMx110EB-AF
CPU	8-core	6-core	4- Core
Intel	XEON® W-11865MRE	XEON® W-11555MRE	XEON® W-11155MRE
CPU TDP	45 / 35 W	45 / 35 W	45 / 35 W
CPU Clock (Base)	2.4 GHz	2.6 GHz	2.4 GHz
L2 Cache	24 MB	12 MB	8 MB
Heat spreader	TQMx110EB-HSP-AA	TQMx110EB-HSP-AA	TQMx110EB-HSP-AA
Heatsink incl. fan	TQMx110EB-KK-AA	TQMx110EB-KK-AA	TQMx110EB-KK-AA
DRAM / SO-DIMM	16 / 32 / 64 GB	16 / 32 / 64 GB	16 / 32 / 64 GB
DRAM / ECC	Yes	Yes	Yes
Use Condition	Embedded w/Turbo ON Industrial w/Turbo OFF	Embedded w/Turbo ON Industrial w/Turbo OFF	Embedded w/Turbo ON Industrial w/Turbo OFF
Operating Temperature	-40 °C to +60 °C (Turbo ON) -40 °C to +75 °C (35 W Turbo OFF)	-40 °C to +60 °C (Turbo ON) -40 °C to +75 °C (35 W Turbo OFF)	-40 °C to +60 °C (Turbo ON) -40 °C to +75 °C (35 W Turbo OFF)
M.2 BGA SSD PCIe x4	--	--	--
TPM 2.0	1	1	1
Independent displays	4	4	4
LVDS or eDP	1	1	1
DP or HDMI	3	3	3
2.5 GbE	1	1	1
USB 2.0 host	8	8	8
USB 3.2 host	4	4	4
SATA Gen 3	4	4	4
PCIe Gen 3 ×1	8	8	8
PEG Gen 4 x16	1	1	1
I2C / SPI	1 / 1	1 / 1	1 / 1
HDA	1	1	1
LPC or eSPI	1	1	1
UART / GPIO	2 / 8	2 / 8	2 / 8

Table 4: TQMx110EB 11th Generation Intel® XEON® H Low Power Embedded Series configurations and features

Feature	TQMx110EB-AG	TQMx110EB-AH	TQMx110EB-AI
CPU	8-core	6-core	4- Core
Intel	XEON® W-11865MLE	XEON® W-11555MLE	XEON® W-11155MLE
CPU TDP	25 W	25 W	25 W
CPU Clock (Base)	1.5 GHz	1.9 GHz	1.8 GHz
L2 Cache	24 MB	12 MB	8 MB
Heat spreader	TQMx110EB-HSP-AA	TQMx110EB-HSP-AA	TQMx110EB-HSP-AA
Heatsink incl. fan	TQMx110EB-KK-AA	TQMx110EB-KK-AA	TQMx110EB-KK-AA
DRAM / SO-DIMM	16 / 32 / 64 GB	16 / 32 / 64 GB	16 / 32 / 64 GB
DRAM / ECC	Yes	Yes	Yes
Use Condition	Embedded w/Turbo ON Industrial w/Turbo OFF	Embedded w/Turbo ON Industrial w/Turbo OFF	Embedded w/Turbo ON Industrial w/Turbo OFF
Operating Temperature	0 °C to +60 °C (Turbo ON) 0 °C to +75 °C (Turbo OFF) *	0 °C to +60 °C (Turbo ON) 0 °C to +75 °C (Turbo OFF)*	0 °C to +60 °C (Turbo ON) 0 °C to +75 °C (Turbo OFF)*
M.2 BGA SSD PCIe x4	--	--	--
TPM 2.0	1	1	1
Independent displays	4	4	4
LVDS or eDP	1	1	1
DP or HDMI	3	3	3
2.5 GbE	1	1	1
USB 2.0 host	8	8	8
USB 3.2 host	4	4	4
SATA Gen 3	4	4	4
PCIe Gen 3 ×1	8	8	8
PEG Gen 4 x16	1	1	1
I2C / SPI	1 / 1	1 / 1	1 / 1
HDA	1	1	1
LPC or eSPI	1	1	1
UART / GPIO	2 / 8	2 / 8	2 / 8

*optional -40° C to +75 °C with screening

Please refer to www.tq-group.com/ for a full list of standard versions.
Other configurations are available on request.

Hardware and software configuration features on request:

- Conformal coating
- Customized BIOS
- Ultra-deep power state Green ECO-Off feature

2.4 Accessories

- **TQMx110EB-HSP**
  Heat spreader for TQMx110EB, according to COM Express™ specification.

- **Evaluation platform MB-COME6-4**
  Mainboard for COM Express™ Basic and Compact, Type 6, 170 × 170 mm², with the following interfaces:
  - 3 × DP (2x up to 8k HBR3, 1x up to 4k HBR2)
  - 1 x dual LVDS
  - 1 x eDP (up to 4k HBR2)
  - 2 × 2.5 Gbit Ethernet
  - 2 x USB 3.2 USB-A
  - 1 x USB 3.2 USB-C
  - 3 x USB 2.0 internal
  - 2 × Serial Port RS232
  - 1x High Definition Audio (Line In, MIC In, HP Out)
  - 1x M.2 Socket Key E (Wi-Fi/BT),
  - 1x M.2 Socket Key B with µSIM (WWAN or SATA SSD)
  - 1x M.2 Socket Key M PCIe x4 (SSD)
  - 1x M.2 Socket Key M PCIe x2 (SSD)
  - 1x PCIExpress x16 PEG port
  - 1x SATA connector
  - Fan header
  - Debug header

- **Debug module**
  POST debug card for TQMx110EB, see3.6.3.

3. FUNCTION

3.1 Block Diagram

The following figure shows the TQMx110EB block diagram.

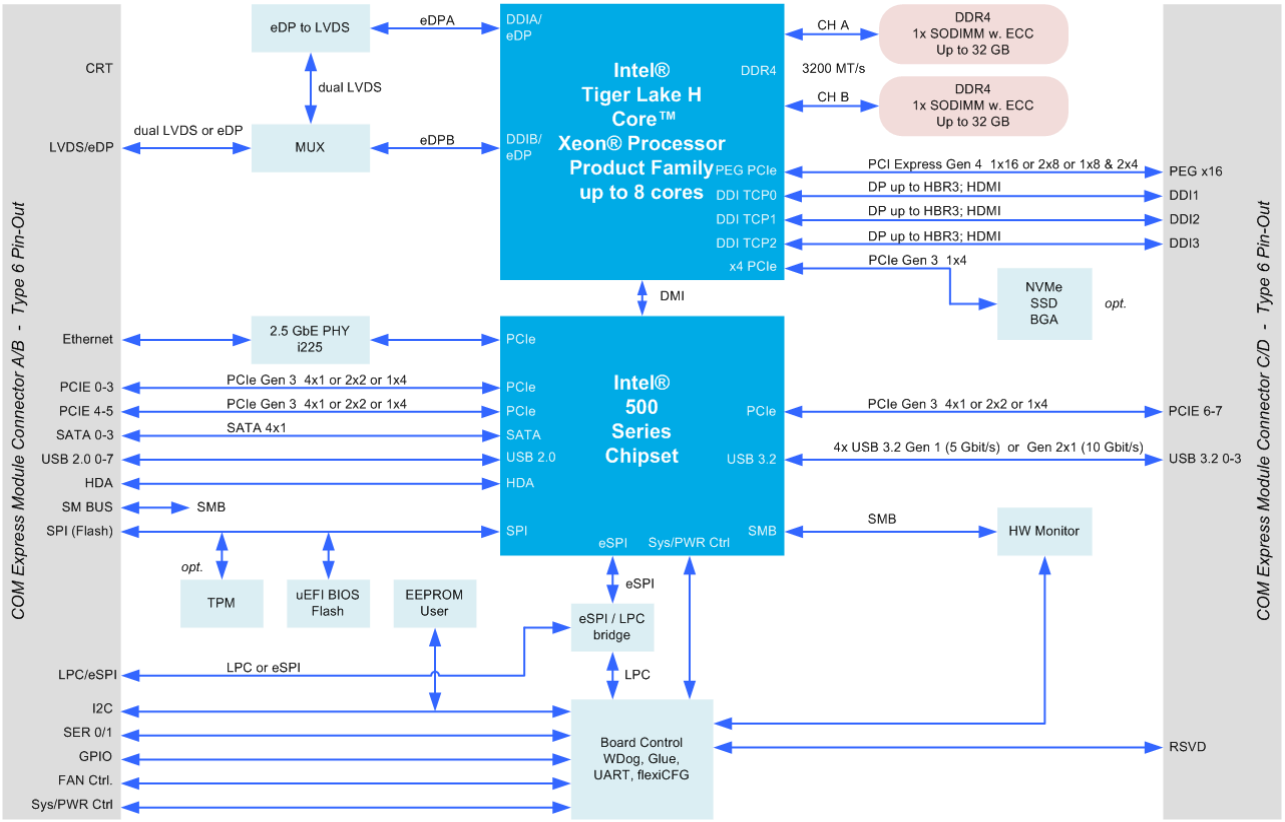


Figure 1: TQMx110EB block diagram

3.2 Electrical Characteristics

3.2.1 Supply Voltage

The TQMx110EB supports a voltage inputs from 11.4 V to 12.6 V.

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

Standard input:	11.4 V to 12.6 V	maximum input ripple:	±100 mV
VCC_5V_SBY:	4.75 V to 5.25 V	maximum input ripple:	±50 mV
VCC_RTC:	2.0 V to 3.3 V	maximum input ripple:	±20 mV

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

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 power consumption values below show the TQMx110EB voltage and power specifications.

The values were measured with two power supplies; one for the TQMx110EB and the other one for the MB-COME6-4 COM Express™ carrier board.

The power consumption of each TQMx110EB version was measured running Windows® 10, 64-bit and a dual DDR4 SO-DIMM configuration (2 × 16 Gbyte). All measurements were done at a temperature of +25 °C and an input voltage of +12 V.

The power consumption of the TQMx110EB depends on the application, the mode of operation and the operating system.

The power consumption was measured under the following test modes:

- **Green ECO-Off state:**
  The system is in Green ECO-Off state, all DC/DC power supplies on the TQMx110EB are switched off.
- **Suspend mode:**
  The system is in S5/S4 state, Ethernet port is disconnected.
- **Windows® 10, 64-bit, idle state:**
  Desktop idle state, Ethernet port is disconnected.
- **Windows® 10, 64-bit, maximum workload (cTDP down mode enabled):**
  These values show the maximum cTDP down power consumption using the Intel® stress test tool to stress the processor and graphic engine. Ethernet port is connected (1000Base-T Speed).
- **Windows® 10, 64-bit, maximum workload (nominal configuration):**
  These values show the maximum worst case power consumption using the Intel® stress test tool to stress the processor and graphic engine. Ethernet port is connected (1000Base-T Speed).
- **Windows® 10, 64-bit, maximum workload (turbo mode first 28 seconds)**
  These values show the maximum worst case power consumption using the Intel® stress test tool to stress the processor and graphic engine. This value was measured only for a short time (28 s) when the processor is in the turbo mode. This value should be used for designing the power supply for the TQMx110EB. Ethernet port is connected (1000Base-T Speed).

The following table shows the TQMx110EB power consumption with different CPUs.

Table 5: TQMx110EB Power Consumption **Turbo Mode ON**

CPU	Mode					
	Standby 5 V		Input 12 V			
	Green ECO-Off state	Suspend	Win10, 64-bit idle	Win10, 64-bit cTDP down max. load	Win10, 64-bit nominal max. load	Win10, 64-bit Max load (Turbo mode)
i7-11850HE	3.5 mW	400 mW	12 W	52 W	63 W	127 W
i5-11500HE	3.5 mW	400 mW	11 W	46 W	58 W	87 W
i3-11100HE	3.5 mW	400 mW	11 W	45 W	55 W	73 W
W-11865MRE	3.5 mW	400 mW	12 W	52 W	63 W	127 W
W-11555MRE	3.5 mW	400 mW	11 W	46 W	58 W	87 W
W-11155MRE	3.5 mW	400 mW	11 W	45 W	55 W	73 W
W-11865MLE	3.5 mW	400 mW	11 W	--	37 W	111 W
W-11555MLE	3.5 mW	400 mW	10 W	--	36 W	86 W
W-11155MLE	3.5 mW	400 mW	10 W	--	34 W	71 W

Table 6: TQMx110EB Power Consumption **Turbo Mode OFF**

CPU	Mode					
	Standby 5 V		Input 12 V			
	Green ECO-Off state	Suspend	Win10, 64-bit idle	Win10, 64-bit cTDP down max. load	Win10, 64-bit nominal max. load	Win10, 64-bit Max load (Turbo mode)
i7-11850HE	3.5 mW	400 mW	12 W	40 W	51 W	--
i5-11500HE	3.5 mW	400 mW	11 W	37 W	47 W	--
i3-11100HE	3.5 mW	400 mW	11 W	36 W	46 W	--
W-11865MRE	3.5 mW	400 mW	12 W	40 W	51 W	--
W-11555MRE	3.5 mW	400 mW	11 W	37 W	47 W	--
W-11155MRE	3.5 mW	400 mW	11 W	36 W	46 W	--
W-11865MLE	3.5 mW	400 mW	11 W	--	30 W	--
W-11555MLE	3.5 mW	400 mW	10 W	--	29 W	--
W-11155MLE	3.5 mW	400 mW	10 W	--	28 W	--

Note: Power requirement	
	The power supplies on the carrier board for the TQMx110EB have to be designed with enough reserve. The carrier board should be able to provide at least twice the maximum TQMx110EB workload power. The TQMx110EB supports several low-power states. The carrier board power supply has to be stable, even with no load. Carrier power supply example: Processor i7-11850HE max. load Turbo ON Power Consumption = 127 W **carrier power design 200 W** Processor i7-11850HE max. load Turbo OFF Power Consumption = 51 W **carrier power design 100 W**

3.2.3 Real Time Clock Power Consumption

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

Table 7: RTC Current Consumption

Mode	Voltage	Current
11th Generation Intel® Core™ and XEON® H series integrated RTC	3.0 V	2 µA

The current consumption of the RTC in the 11th Generation Intel® Core™ and XEON® H series Product Family Datasheet is specified with 6 µA in average, but the measured values on several TQMx110EB are lower.

3.3 Environmental Conditions

- Operating Standard temperature: 0 °C to +60 °C
- Operating Extended temperature: –40 °C to +75 °C
- Storage temperature: –40 °C to +85 °C
- Relative humidity (operating): 10 % to 90 % (non-condensing)
- Relative humidity (storage): 5 % to 95 % (non-condensing)

Table 8: Operating Temperature

CPU	0 °C to +60 °C	0 °C to +75 °C	-40 °C to +60 °C	-40 °C to +75 °C
i7-11850HE	45 W / Turbo ON	35 W / Turbo OFF	--	--
i5-11500HE	45 W / Turbo ON	35 W / Turbo OFF	--	--
i3-11100HE	45 W / Turbo ON	35 W / Turbo OFF	--	--
W-11865MRE	45 W / Turbo ON	35 W / Turbo OFF	45 W / Turbo ON	35 W / Turbo OFF
W-11555MRE	45 W / Turbo ON	35 W / Turbo OFF	45 W / Turbo ON	35 W / Turbo OFF
W-11155MRE	45 W / Turbo ON	35 W / Turbo OFF	45 W / Turbo ON	35 W / Turbo OFF
W-11865MLE	25 W / Turbo ON	25 W / Turbo OFF	(optional with screening)	(optional with screening)
W-11555MLE	25 W / Turbo ON	25 W / Turbo OFF	(optional with screening)	(optional with screening)
W-11155MLE	25 W / Turbo ON	25 W / Turbo OFF	(optional with screening)	(optional with screening)

Attention: Maximum operating temperature	
	Do not operate the TQMx110EB without properly attached heat spreader and heat sink. The heat spreader is not a sufficient heat sink.

3.4 System Components

3.4.1 Processor

The TQMx110EB supports the 11th Generation Intel® Core™ and XEON® H processor series (TigerLake-H).

The following list illustrates some key features of the 11th Generation Intel® Core™ and XEON® H processor series:

- 8-core, 6-core and 4-core processor cores
- 10nm SuperFin technology processor up to 24MB LLC / 14nm PCH
- DDR4 up to 3200 MT/s optional with ECC (XEON® H versions only)
- Intel® Hyper-Threading Technology (Intel® HT Technology)
- Intel® Advanced Vector Extensions 512 Bit (Intel® AVX-512)
- Intel® Transactional Synchronization Extensions (Intel® TSX-NI)
- Intel® 64 Architecture
- Intel® Turbo Boost Max Technology 3.0
- Intel® Configurable Thermal Design Power (Intel® cTDP down)
- Intel® Enhanced Intel® SpeedStep® technology
- Intel® Iris®Xe Graphics
- High Definition Content Protection (HDCP) 2.3
- Four independent displays

Table 9: 11th Generation Intel® Core™ i7, i5, i3 Embedded Series

Mode	Core™ i7-11850HE	Core™ i5-11500HE	Core™ i3-11100HE
Processor Cores / Threads	8 / 16	6 / 12	4 / 8
Cache	24 Mbyte	12 Mbyte	8 Mbyte
Core Base frequency	2.6 GHz	2.6 GHz	2.4 GHz
Core Base frequency (cTDP down)	2.1 GHz	2.1 GHz	1.9 GHz
Core Max. Turbo frequency	4.7 GHz	4.5 GHz	4.4 GHz
$T_{junction}$	0 °C to +100 °C	0 °C to +100 °C	0 °C to +100 °C
Memory speed DDR4	3200 MT/s	3200 MT/s	3200 MT/s
Max. memory	64 Gbyte	64 Gbyte	64 Gbyte
Memory configuration	Dual, no ECC	Dual, no ECC	Dual, no ECC
Graphics	Intel® Iris®Xe Graphics	Intel® Iris®Xe Graphics	Intel® Iris®Xe Graphics
Graphics Execution Units	32	32	16
Graphics Base frequency	0.35 GHz	0.35 GHz	0.35 GHz
Graphics Turbo frequency	1.35 GHz	1.35 GHz	1.25 GHz
Thermal Design Power (TDP nominal)	45 W	45 W	45 W
Configurable Thermal Design Power (cTDP down)	35 W	35 W	35 W
Processor Power Limit 2 (PL2)	109 W	83 W	65 W
Intel® Hyper-Threading Technology	Yes	Yes	Yes
Intel® Turbo Boost Technology	Yes	Yes	Yes
TSN support	No	No	No
Chipset	HM570E	HM570E	HM570E

Table 10: 11th Generation Intel® XEON® Embedded Series

Mode	XEON® W-11865MRE	XEON® W-11555MRE	XEON® W-11155MRE
Processor Cores / Threads	8 / 16	6 / 12	4 / 8
Cache	24 Mbyte	12 Mbyte	8 Mbyte
Core Base frequency	2.6 GHz	2.6 GHz	2.4 GHz
Core Base frequency (cTDP down)	2.1 GHz	2.1 GHz	1.9 GHz
Core Max. Turbo frequency	4.7 GHz	4.5 GHz	4.4 GHz
$T_{junction}$	-40 °C to +100 °C	-40 °C to +100 °C	-40 °C to +100 °C
Memory speed DDR4	3200 MT/s	3200 MT/s	3200 MT/s
Max. memory	64 Gbyte	64 Gbyte	64 Gbyte
Memory configuration	Dual, with ECC	Dual, with ECC	Dual, with ECC
Graphics	Intel® Iris®Xe Graphics	Intel® Iris®Xe Graphics	Intel® Iris®Xe Graphics
Graphics Execution Units	32	32	16
Graphics Base frequency	0.35 GHz	0.35 GHz	0.35 GHz
Graphics Turbo frequency	1.35 GHz	1.35 GHz	1.25 GHz
Thermal Design Power (TDP nominal)	45 W	45 W	45 W
Configurable Thermal Design Power (cTDP down)	35 W	35 W	35 W
Processor Power Limit 2 (PL2)	109 W	83 W	65 W
Intel® Hyper-Threading Technology	Yes	Yes	Yes
Intel® Turbo Boost Technology	Yes	Yes	Yes
TSN support	Yes	Yes	Yes
Chipset	RM590E	RM590E	RM590E

Table 11: 11th Generation Intel® XEON® Low Power Embedded Series

Mode	XEON® W-11865MLE	XEON® W-11555MLE	XEON® W-11155MLE
Processor Cores / Threads	8 / 16	6 / 12	4 / 8
Cache	24 Mbyte	12 Mbyte	8 Mbyte
Core Base frequency	1.5 GHz	1.9 GHz	1.8 GHz
Core Base frequency (cTDP down)	--	--	--
Core Max. Turbo frequency	4.5 GHz	4.4 GHz	3.1 GHz
$T_{junction}$	0 °C to +100 °C	0 °C to +100 °C	0 °C to +100 °C
Memory speed DDR4	3200 MT/s	3200 MT/s	3200 MT/s
Max. memory	64 Gbyte	64 Gbyte	64 Gbyte
Memory configuration	Dual, with ECC	Dual, with ECC	Dual, with ECC
Graphics	Intel® Iris®Xe Graphics	Intel® Iris®Xe Graphics	Intel® Iris®Xe Graphics
Graphics Execution Units	32	32	16
Graphics Base frequency	0.35 GHz	0.35 GHz	0.35 GHz
Graphics Turbo frequency	1.35 GHz	1.35 GHz	1.25 GHz
Thermal Design Power (TDP nominal)	25 W	25 W	25 W
Configurable Thermal Design Power (cTDP down)	--	--	--
Processor Power Limit 2 (PL2)	109 W	89 W	57 W
Intel® Hyper-Threading Technology	Yes	Yes	Yes
Intel® Turbo Boost Technology	Yes	Yes	Yes
TSN support	Yes	Yes	Yes
Chipset	RM590E	RM590E	RM590E

3.4.1.1 Intel® Turbo Boost Technology

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

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

The Intel® Turbo Boost Technology can be configured in the uEFI BIOS, the default setting is “enabled”.

Only the Intel® Core™ i7, i5, i3 and XEON® processors support Intel® Turbo Boost Technology.

3.4.1.2 Intel® Configurable Thermal Design Power

The Intel® Configurable Thermal Design Power (cTDP) feature allows adjustment of the processor power consumption.

The cTDP consists of three modes:

1. The cTDP nominal mode specifies the processor rated frequency and power consumption.
2. The cTDP down mode specifies a lower processor power consumption and lower guaranteed frequency versus the nominal mode. This mode can be selected for ultra low-power applications, e.g. systems with reduced cooling solutions.

The cTDP up feature (35 W) is only available on the 11th Generation Intel® Core™ and XEON® H processor versions with 45 W TDP.

The cTDP function can be configured in the uEFI BIOS. The default setting is “nominal”.

3.4.2 Graphics

The 11th Generation Intel® Core™ and XEON® H series includes an integrated Intel® HD graphics accelerator.

It provides excellent 2D / 3D graphics performance with support of four simultaneous displays.

The following list illustrates some key features of the 11th Generation Intel® Core™ and XEON® H processor:

- Intel® Iris®Xe Graphics with 32 Execution Units
- Hardware accelerated video decoding/encoding for AVC/VC-1/MPEG2/HEVC/VP8/JPEG
- Direct3D11 Video API support
- OpenGL 4.5
- Open CL 2.1, Open CL 2.0, Open CL 1.2
- Single 8K60Hz (HBR3) panel support

The TQMx110EB supports three external Digital Display Interfaces (DDI1, DDI2 and DDI3) and one internal display, either dual channel LVDS or eDP interface at the COM Express™ connector, depending on TQMx110EB and carrier configuration.

The 11th Generation Intel® Core™ and XEON® H series supports up to four displays at the same time.

Table 12: Maximum Resolution Display Configuration

Display	Maximum Display Resolution
LVDS	1920 × 1200 @ 60 Hz
eDP 1.4b	4096 × 2304 @ 60 Hz
DP 1.4a	7680 × 4320 @ 60 Hz
HDMI 2.0b	4096 × 2160 @ 60 Hz

3.4.3 Chipset

The 11th Generation Intel® Core™ and XEON® H processor series includes the embedded Intel® RM590 and HM570 platform controller hub (PCH).

3.4.4 Memory

3.4.4.1 DDR4 SDRAM SO-DIMM

The TQMx110EB supports a dual-channel DDR4 memory with optional error-correcting code (ECC), running at up to 3200 MT/s.
It provides two 260-pin DDR4 SO-DIMM sockets for two DDR4 SO-DIMM modules that support system memory configurations of 16 Gbyte, 32 Gbyte or 64 Gbyte.
The ECC feature can only be used with the 11th Generation Intel® XEON H processor combined with the Intel® RM590 PCH.

Note: DDR4 SO-DIMM modules	
	Only DDR4 SO-DIMM modules qualified by TQ-Systems are authorized for use with the TQMx110EB. DDR4 SO-DIMM modules not released by TQ-Systems may cause functional issues.

3.4.4.2 M.2 BGA SSD

The TQMx110EB supports an on-board M.2 BGA SSD flash device.
The M.2 BGA SSD device capacity is available from 30 Gbyte up to 1 Tbyte. The new M.2 BGA SSD offering a PCI Express Gen 3 x4 high speed interface supporting the NVMe protocol that is designed to address the needs of the industrial segment: longevity, reliability, quality and ruggedness.

Benefits of the M.2 BGA SSD

- High integration (single chip BGA)
- High speed interface PCI Express Gen 3 x4 (if M.2 BGA chips available Gen 4)
- Robust design optimized for rugged application
- Extended temperature ranges available (industrial and automotive)
- Intelligent power fail protection and recovery protects data from unexpected power loss
- Low power consumption
- Robust data security
- Sophisticated wear leveling and bad block management
- Pseudo Single Level Cell (pSLC) configuration available for high endurance

3.4.4.3 SPI Boot Flash

The TQMx110EB provides a 256 Mbit SPI boot flash. It includes the Intel® Management Engine (Intel® ME) and the uEFI BIOS.
An external SPI boot flash on the carrier can be used instead of the on-board SPI boot flash.
The uEFI BIOS supports the following 3.3 V SPI flash devices on the carrier board:

- Macronix MX25L25645GM2I

3.4.4.4 EEPROM

The TQMx110EB supports a COM Express™ Module EEPROM. The 2 kbit EEPROM AT24AA32 is connected to the general purpose I^2C interface (COM Express™ pin names I2C_DAT and I2C_CK).

3.4.5 Real Time Clock

The TQMx110EB includes a standard RTC (Motorola MC146818B) integrated in the Intel PCH.

3.4.6 Trusted Platform Module

The TQMx110EB supports the Trusted Platform Module (TPM) 2.0 (Infineon SLB9670 controller).
The 11th Generation Intel® Core™ and XEON® H series also support a Firmware Trusted Platform Module (FTPM), which is a Trusted Platform Module 2.0 implementation in firmware. This feature can be configured in the BIOS.

3.4.7 Hardware Monitor

The TQMx110EB includes an integrated Hardware Monitor to monitor the on-board and processor die temperature, board voltages and manage the fan control of the COM Express™ interface.

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

The TQ-Systems COM Express™ module TQMx110EB includes a flexible I/O configuration feature, 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 TQMx110EB to reduce the carrier board design effort. Some examples of flexible I/O configuration are:

- GPIO interrupt configuration
- Interrupt configuration via LPC Serial IRQ
- Serial Port handshake signals via GPIOs
- Integration of 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.

3.4.9 Ultra Deep Power State Green ECO-Off (optional)

The TQMx110EB supports the ultra-deep power state Green ECO-Off. In this configuration all DC/DC power supplies on the TQMx110EB 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 has to be pulled low for at least 100 msec.

3.5 Interfaces

3.5.1 PCI Express

The TQMx110EB supports up to eight PCI Express Gen 3 ports with 8 Gb/s speed at the COM Express™ connector port 0 – 3 and 4 – 7.

With a customized BIOS the PCI Express lane configuration can be set as follows:

Table 13: PCI Express port 0 – 7 Configuration Options

COM Express™ Port 0 – 3	Configuration
(4) ×1 ports	Standard BIOS
(1) ×2 and (2) ×1 ports	Configuration via custom BIOS
(1) ×4 port	Configuration via custom BIOS
COM Express™ Port 4 – 7	**Configuration**
(4) ×1 ports	Configuration via custom BIOS
(1) ×2 and (2) ×1 ports	Configuration via custom BIOS
(1) ×4 port	Standard BIOS

The PCI Express COM Express™ connector port 4 to 7 supports a flexible I/O configuration to directly connect an M.2 SSD module with PCI Express 1 (×4) interface.

To support Intel® Optane™ or Rapid Storage Technology, the four PCI Express lanes of the 11th Generation Intel® Core™ and XEON® H series are connected to COM Express™ connector port 4 to 7 and used on an M.2 PCI Express socket.

3.5.2 PCI Express for Graphics (PEG)

At the COM Express™ connector PEG interface the TQMx110EB supports one Gen 4 PCI Express Graphics port with 16.0 Gb/s speed.

The default configuration for the PCI Express Graphic lanes is 1 (×16). In the BIOS the PCI Express Graphic lanes can be configured to 1 (×16), 2 (×8) or 2 (×4) + 1 (×8). This configuration increases the number of available PCI Express lanes.

The PCI Express Graphic port can be used for PCI Express graphics devices or high speed non-graphic PCI Express devices (e.g. quad Gigabit Ethernet or 10 Gigabit Ethernet controller).

Attention: PCI Express Gen 4 carrier design	
	The COM Express™ specification Revision 3.0 only supports the PCI Express Gen 3 (8 Gb/s) data rate. If the COM Express™ carrier is not designed for the PCI Express Gen 4 (16 Gb/s) operation, the PCI Express port should be configured to operate in Gen 3 (8 Gb/s) mode.

3.5.3 Gigabit Ethernet

The TQMx110EB provides an Intel® i225 Ethernet controller with 10/100/1000/2500 Mbps speed.

Features of the Intel® i225 Ethernet controller:

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

Attention: 2500 BASE-T Ethernet carrier design	
	The COM Express™ specification Revision 3.0 only supports the Gigabit Ethernet 1000 BASE-T data rate. If the COM Express™ carrier is not designed for the Gigabit Ethernet 2500 BASE-T operation, the Gigabit Ethernet ports should be configured to operate in 1000 BASE-T mode.

3.5.4 Serial ATA

The TQMx110EB supports four SATA Gen 3.0 (6 Gbit/s) interfaces. The integrated SATA host controller supports AHCI mode and it also supports RAID mode.
The SATA controller no longer supports legacy IDE mode using I/O space.

The RAID capability provides high-performance RAID 0, 1, 5, and 10 functionality on up to four SATA ports of the SATA host controller. Matrix RAID support is provided to allow multiple RAID levels to be combined on a single set of hard drives, such as RAID 0 and RAID 1 on two disks. Other RAID features include hot spare support, SMART alerting, and RAID 0 auto replace.

To support more PCI Express ports the four SATA ports can be configured to four PCI Express ports with Gen 3 (8 Gb/s) data rate.

Please contact support@tq-group.com for further information about the SATA / PCI Express port configuration.

3.5.5 Digital Display Interface

The TQMx110EB supports four Digital Display Interfaces at the COM Express™ connector DDI1, DDI2, DDI3 and eDP / LVDS port.

The external Digital Display Interface supports Display Port (DP), High Definition Multimedia Interface (HDMI) and Digital Visual Interface (DVI). Any display combination is supported.

The internal eDP / LVDS port supports LVDS (via an eDP to LVDS Bridge)

Maximum display resolutions:

- DisplayPort 1.4a resolution up to 7680 × 4320 @ 60 Hz
- HDMI 2.0b up to 4096 × 2160 @ 60 Hz
- DVI up to 4096 × 2160 @ 24 Hz (HDMI without Audio)
- eDP up to 4 lanes eDP 1.4b up to 4096 × 2304 @ 60 Hz
- LVDS up to 1920 × 1200 @ 60 Hz in dual channel LVDS mode

3.5.6 LVDS / eDP Interface

The TQMx110EB supports a LVDS / eDP interface at the COM Express™ connector. The LVDS interface is provided through an on-board eDP to LVDS Bridge. The eDP to LVDS Bridge supports single or dual bus LVDS signalling with colour depths of 18 bits per pixel or 24 bits per pixel up to 112 MHz and a resolution up to 1920 × 1200 @ 60 Hz in dual channel LVDS mode.

The TQMx110EB includes a multiplexer to switch between the LVDS and the eDP interface on the COM Express™ connector pins. In the BIOS the LVDS or eDP interface can be configured.

The LVDS data output 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.

3.5.7 USB Interfaces

The TQMx110EB supports eight USB 2.0 and four USB 3.2 Gen 2 ports with data rate up to 10 Gb/s at the COM Express™ connector. All USB 3.2 Gen 2 ports are configurable to USB 3.2 Gen 1 (5 Gb/s).
Care must be taken in the COM Express™ carrier design, the carrier must support the USB 3.2 Gen 2 (10 Gb/s) high speed standard.

Attention: USB 3.1 Gen 2 (10 Gb/s) carrier design	
	The COM Express™ specification Revision 3.0 only supports the USB 3.2 Gen 1 (5 Gb/s) data rate. If the COM Express™ carrier is not designed for the USB 3.2 Gen 2 (10 Gb/s) operation, the USB 3.2 ports should be configured to operate in Gen 1 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. The USB 2.0 port 2 must be paired with USB 3.2 SuperSpeedPlus port 2. The USB 2.0 port 3 must be paired with USB 3.2 SuperSpeedPlus port 3.

3.5.8 General Purpose Input / Output

The TQMx110EB provides eight GPIO signals at the COM Express™ connector. The GPIO signals are shared with the SD card signals. The GPIO signals are integrated in the TQ-flexiCFG block and can be configured flexibly.
The signals can also be used for special functions (see 3.4.8).

3.5.9 High Definition Audio Interface

The TQMx110EB provides a High Definition Audio (HDA) interface, which supports two audio codecs at the COM Express™ connector. The HDA_SDIN2 signal at the COM Express™ connector is not connected. The Audio Codec is assembled on the carrier board.

3.5.10 LPC / eSPI Bus

The TQMx110EB supports a Low Pin Count (LPC) legacy bus and the Enhanced Serial Peripheral (eSPI) bus on the same COM Express™ connector pins.
The TQMx110EB includes a multiplexer to switch between the LPC 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.

The default COM Express™ interface configuration is LPC bus. For the eSPI option a BIOS configuration is necessary.

Please contact support@tq-group.com for further information about the Serial Peripheral eSPI BIOS and Carrier integration.

3.5.11 I²C Bus

The TQMx110EB supports a general purpose I²C port via a dedicated LPC to I²C controller integrated in the TQ-flexiCFG block.
The I²C host controller supports a transfer rate of up to 400 kHz and can be configured independently.

3.5.12 SMBus

The TQMx110EB provides a System Management Bus (SMBus).

3.5.13 Serial Peripheral Interface

The TQMx110EB provides a Serial Peripheral Interface (SPI) interface.
The SPI interface can only be used for SPI boot Flash devices.

3.5.14 Serial Ports

The TQMx110EB 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 14: Serial Port COM Express™ Port Mapping

COM Express™ Signal	COM Express™ Pin	TQMx110EB	Remark
SER0_TX	A98	SER0_TX	3.3 V output (without protection)
SER0_RX	A99	SER0_RX	3.3 V input (without protection)
SER1_TX	A101	SER1_TX	3.3 V output (without protection)
SER1_RX	A102	SER1_RX	3.3 V input (without protection)
SER0_RTS#	B98	SER0_RTS#	3.3 V output
SER0_CTS#	B99	SER0_CTS#	3.3 V input
SER1_RTS#	D24	SER1_RTS#	3.3 V output
SER1_CTS#	D25	SER1_CTS#	3.3 V input

Note: Protection circuits	
	In COM Express™ specification Revision 3.0 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 exposed to 12 V. The implementation of this circuitry causes lower transfer rates on the two serial ports. On the TQMx110EB the protection circuit is removed by default and the serial ports provide transfer rates of up to 115 kbaud. Therefore the TQMx110EB can only be used in a COM Express™ COM.0 2.0 and 3.0 Type 6 pin-out carrier board.

3.5.15 Watchdog Timer

The TQMx110EB supports an independently programmable two-stage Watchdog timer integrated in the TQ-flexiCFG block.

There are four operation modes available for the Watchdog timer:

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

The Watchdog timer timeout ranges from 125 msec to 1 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

3.6.1 COM Express™ Connector

Two 220-pin 0.5 mm pitch receptacle connectors are used to interface the TQMx110EB on the carrier board.
On the carrier board two 220-pin 0.5 mm pitch plug connectors have to be used.
Two versions with 5 mm and 8 mm stack height are available.

Attention: USB 3.1 Gen 2 (10 Gb/s), PCI Express Gen 4 (16 Gb/s) and DisplayPort HBR3 (8.1 GB/s) carrier design	
	The COM Express™ specification Revision 3.0 only supports the USB 3.2 Gen 1 (5 Gb/s), PCI Express Gen 3 (8 Gb/s) and DisplayPort HBR2 (5.4 Gb/s) data rate. To support on the COM Express™ carrier the new high speed interfaces, USB 3.2 Gen 2 (10 Gb/s), PCI Express Gen 4 (16 Gb/s) and DisplayPort HBR3 (8.1 Gb/s) data rate, a COM Express™ optimized high speed connector must be used. The company EPT offers an optimized COM Express™ connector (Colibri) for applications up to 16 Gb/s, this connector is compatible with all popular COM Express™ connectors. The Carrier design also needs to be optimized to support the new high speed interfaces. Please contact support@tq-group.com for further information about the new high speed design requirements

3.6.2 Debug Header

The TQMx110EB includes a 14-pin flat cable connector to connect an external debug module (TQ specific) providing uEFI BIOS POST code information, debug LEDs and a JTAG interface for on-board FPGA.
The TQM debug card can be connected at this header.

3.6.3 TQM Debug Card

The TQM debug card is 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.

Figure 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 Module LED

The TQMx110EB includes a dual colour LED providing boot and BIOS information.
The following table illustrates some LED boot messages:

Table 15: LED Boot Messages

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

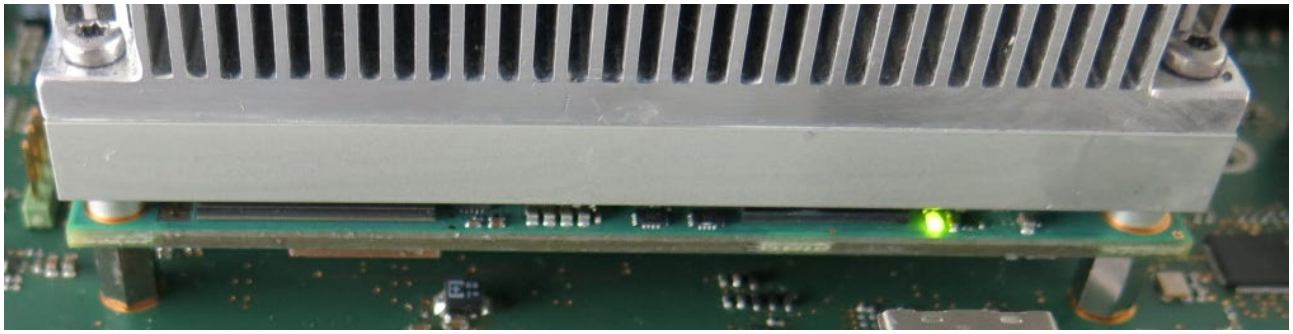


Figure 3: Debug Module LED

3.7 COM Express™ Connector Pinout

This section describes the TQMx110EB COM Express™ connector pin assignment, which is compliant with COM.0 R3.0 Type 6 pin-out definitions.

3.7.1 Signal Assignment Abbreviations

The following table lists the abbreviations used within this chapter:

Table 16: Signal Assignment Abbreviations

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
I/O	Bi-directional

Note: Unused signals on the carrier board	
	Unused inputs at the COM Express™ connector can be left open on the carrier board, since these signals are terminated on the TQMx110EB.

3.7.2 COM Express™ Connector Pin Assignment

Table 17: 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 / 2500 Mbit/s link indicator	OD	
A5	GBE0_LINK1000#	Gigabit Ethernet Controller 0 1000 Mbit/s 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. Active low output.	O PD	TQ-flexiCFG
A16	SATA0_TX+	SATA differential transmit pairs	O	
A17	SATA0_TX-	SATA differential transmit pairs	O	
A18	SUS_S4#	Indicates system is in Suspend to Disk state. Active low output.	O PD	TQ-flexiCFG
A19	SATA0_RX+	SATA differential receive pairs	I	
A20	SATA0_RX-	SATA differential receive pairs	I	
A21	GND(FIXED)	Ground	GND	
A22	SATA2_TX+	SATA differential transmit pairs	O	
A23	SATA2_TX-	SATA differential transmit pairs	O	
A24	SUS_S5#	Indicates system is in Soft Off state. Active low output.	O PD	TQ-flexiCFG
A25	SATA2_RX+	SATA differential receive pairs	I	
A26	SATA2_RX-	SATA differential receive pairs	I	
A27	BATLOW#	Indicates that external battery is low	I PU	
A28	(S)ATA_ACT#	SATA activity indicator	O	
A29	HDA_SYNC	Sample-synchronization signal to the CODEC(s)	O	
A30	HDA_RST#	Reset output to CODEC, active low.	O	
A31	GND(FIXED)	Ground	GND	
A32	HDA_BITCLK	Serial data clock generated by the external CODEC(s)	IO	
A33	HDA_SDOUT	Serial TDM data output to the CODEC	O	
A34	BIOS_DIS0#/ESPI_SAFS	Selection straps to determine the BIOS boot device	I PU	
A35	THRMTRIP#	indicating that the CPU has entered thermal shutdown	O	
A36	USB6-	USB differential pairs	IO	
A37	USB6+	USB differential pairs	IO	
A38	USB_6_7_OC#	USB over-current sense, USB channels 6 and 7	I PU	
A39	USB4-	USB differential pairs	IO	
A40	USB4+	USB differential pairs	IO	
A41	GND(FIXED)	Ground	GND	
A42	USB2-	USB differential pairs	IO	
A43	USB2+	USB differential pairs	IO	
A44	USB_2_3_OC#	USB over-current sense, USB channels 2 and 3	I PU	
A45	USB0-	USB differential pairs	IO	
A46	USB0+	USB differential pairs	IO	
A47	VCC_RTC	Real-time clock circuit-power input.	Power	
A48	RSVD	Reserved	O	TQ-flexiCFG
A49	GBE0_SDP	Gigabit Ethernet Controller 0 Software-Definable Pin.	IO	TQ-flexiCFG
A50	LPC_SERIRQ/ESPI_CS1#	LPC serial interrupt / eSPI CS1#	IO	3.3V / 1.8V
A51	GND(FIXED)	Ground	GND	
A52	PCIE_TX5+	PCI Express differential transmit pairs	O	
A53	PCIE_TX5-	PCI Express differential transmit pairs	O	
A54	GPI0/SD_DATA0	GPI0	I PU	TQ-flexiCFG
A55	PCIE_TX4+	PCI Express differential transmit pairs	O	

COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
A56	PCIE_TX4-	PCI Express differential transmit pairs	O	
A57	GND	Ground	GND	
A58	PCIE_TX3+	PCI Express differential transmit pairs	O	
A59	PCIE_TX3-	PCI Express differential transmit pairs	O	
A60	GND(FIXED)	Ground	GND	
A61	PCIE_TX2+	PCI Express differential transmit pairs	O	
A62	PCIE_TX2-	PCI Express differential transmit pairs	O	
A63	GPI1/SD_DATA1	GPI1	I PU	TQ-flexiCFG
A64	PCIE_TX1+	PCI Express differential transmit pairs	O	
A65	PCIE_TX1-	PCI Express differential transmit pairs	O	
A66	GND	Ground	GND	
A67	GPI2/SD_DATA2	GPI2	I PU	TQ-flexiCFG
A68	PCIE_TX0+	PCI Express differential transmit pairs	O	
A69	PCIE_TX0-	PCI Express differential transmit pairs	O	
A70	GND(FIXED)	Ground	GND	
A71	LVDS_A0+ / eDP_TX2+	LVDS Channel A differential pairs 0 / eDP_TX2+	O	
A72	LVDS_A0- / eDP_TX2-	LVDS Channel A differential pairs 0 / eDP_TX2-	O	
A73	LVDS_A1+ / eDP_TX1+	LVDS Channel A differential pairs 1 / eDP_TX1+	O	
A74	LVDS_A1- / eDP_TX1-	LVDS Channel A differential pairs 1 / eDP_TX1-	O	
A75	LVDS_A2+ / eDP_TX0+	LVDS Channel A differential pairs 2 / eDP_TX0+	O	
A76	LVDS_A2- / eDP_TX0-	LVDS Channel A differential pairs 2 / eDP_TX0-	O	
A77	LVDS_VDD_EN	LVDS / eDP panel power enable	O PD	
A78	LVDS_A3+	LVDS Channel A differential pairs 3	O	
A79	LVDS_A3-	LVDS Channel A differential pairs 3	O	
A80	GND(FIXED)	Ground	GND	
A81	LVDS_A_CK+ / eDP_TX3+	LVDS Channel A differential clock / eDP_TX3+	O	
A82	LVDS_A_CK- / eDP_TX3-	LVDS Channel A differential clock / eDP_TX3-	O	
A83	LVDS_I2C_CK / eDP_AUX+	I2C clock output for LVDS display / eDP-AUX+	IO	
A84	LVDS_I2C_DAT / eDP_AUX-	I2C data line for LVDS display / eDP_AUX-	IO	
A85	GPI3/SD_DATA3	GPI3 / SD_DATA3	I PU	TQ-flexiCFG
A86	RSVD18	Reserved	NC	
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 Flash	PWR	3.3V
A92	SPI_MISO	Data in to Module from Carrier SPI	I PU	
A93	GPO0/SD_CLK	GPO0	O PD	TQ-flexiCFG
A94	SPI_CLK	Clock from Module to Carrier SPI	O	
A95	SPI_MOSI	Data out from Module to Carrier SPI	O	
A96	TPM_PP	Trusted Platform Module (TPM) Physical Presence pin	I PD	TQ-flexiCFG
A97	TYPE10#	Type 10 Module indication (NC)	NC	
A98	SER0_TX	Serial port 0 transmitter	O	w/o protection 3.3V
A99	SER0_RX	Serial port 0 receiver	I PU	w/o protection 3.3V
A100	GND(FIXED)	Ground	GND	
A101	SER1_TX	Serial port 1 transmitter	O	w/o protection 3.3V
A102	SER1_RX	Serial port 1 receiver	I PU	w/o protection 3.3V
A103	LID#	LID switch	I PU	
A104	VCC_12V	Primary wide power input	PWR	
A105	VCC_12V	Primary wide power input	PWR	
A106	VCC_12V	Primary wide power input	PWR	
A107	VCC_12V	Primary wide power input	PWR	
A108	VCC_12V	Primary wide power input	PWR	
A109	VCC_12V	Primary wide power input	PWR	
A110	GND(FIXED)	Ground	GND	

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 CS0#	IO	3.3V / 1.8V
B4	LPC_AD0/ESPI_IO_0	LPC multiplexed address, command and data bus / eSPI IO0	IO	3.3V / 1.8V
B5	LPC_AD1/ESPI_IO_1	LPC multiplexed address, command and data bus / eSPI IO1	IO	3.3V / 1.8V
B6	LPC_AD2/ESPI_IO_2	LPC multiplexed address, command and data bus / eSPI IO2	IO	3.3V / 1.8V
B7	LPC_AD3/ESPI_IO_3	LPC multiplexed address, command and data bus / eSPI IO3	IO	3.3V / 1.8V
B8	LPC_DRQ0#/ESPI_ALERT0#	LPC serial DMA request / eSPI ALERT0#	IO	3.3V / 1.8V
B9	LPC_DRQ1#/ESPI_ALERT1#	LPC serial DMA request / eSPI ALERT1#	IO	3.3V / 1.8V
B10	LPC_CLK/ESPI_CK	LPC clock output / eSPI Clock	O	3.3V / 1.8V
B11	GND(FIXED)	Ground	GND	
B12	PWRBTN#	Power button input	I PU	TQ-flexiCFG
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 pairs	O	
B17	SATA1_TX-	SATA differential transmit pairs	O	
B18	SUS_STAT#/ESPI_RESET	LPC Indicates suspend operation / eSPI RST#	O	3.3V / 1.8V
B19	SATA1_RX+	SATA differential receive pairs	I	
B20	SATA1_RX-	SATA differential receive pairs	I	
B21	GND(FIXED)	Ground	GND	
B22	SATA3_TX+	SATA differential transmit pairs	O	
B23	SATA3_TX-	SATA differential transmit pairs	O	
B24	PWR_OK	Power OK from main power supply	I PU	TQ-flexiCFG
B25	SATA3_RX+	SATA differential receive pairs	I	
B26	SATA3_RX-	SATA differential receive pairs	I	
B27	WDT	watchdog time-out	O	TQ-flexiCFG
B28	HDA_SDIN2	Serial TDM data input	I PU	N/A
B29	HDA_SDIN1	Serial TDM data input	I PU	
B30	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 I2C port clock output	IO	TQ-flexiCFG
B34	I2C_DAT	General purpose I2C port data I/O line	IO	TQ-flexiCFG
B35	THRM#	Input from carrier temperature sensor	I PU	
B36	USB7-	USB differential pairs	IO	
B37	USB7+	USB differential pairs	IO	
B38	USB_4_5_OC#	USB over-current sense, USB channels 4 and 5	I PU	
B39	USB5-	USB differential pairs	IO	
B40	USB5+	USB differential pairs	IO	
B41	GND(FIXED)	Ground	GND	
B42	USB3-	USB differential pairs	IO	
B43	USB3+	USB differential pairs	IO	
B44	USB_0_1_OC#	USB over-current sense, USB channels 0 and 1	I PU	
B45	USB1-	USB differential pairs	IO	
B46	USB1+	USB differential pairs	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 PU	N/A
B49	SYS_RESET#	Reset button input	I PU	TQ-flexiCFG
B50	CB_RESET#	Reset output from Module to Carrier Board	O	TQ-flexiCFG
B51	GND(FIXED)	Ground	GND	
B52	PCIE_RX5+	PCI Express differential receive pairs	I	
B53	PCIE_RX5-	PCI Express differential receive pairs	I	
B54	GPO1/SD_CMD	GPO1	O PD	TQ-flexiCFG
B55	PCIE_RX4+	PCI Express differential receive pairs	I	

COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
B56	PCIE_RX4-	PCI Express differential receive pairs	I	
B57	GPO2 / SD_WP	GPO2	O PD	TQ-flexiCFG
B58	PCIE_RX3+	PCI Express differential receive pairs	I	
B59	PCIE_RX3-	PCI Express differential receive pairs	I	
B60	GND(FIXED)	Ground	GND	
B61	PCIE_RX2+	PCI Express differential receive pairs	I	
B62	PCIE_RX2-	PCI Express differential receive pairs	I	
B63	GPO3/SD_CD#	GPO3	O PD	TQ-flexiCFG
B64	PCIE_RX1+	PCI Express differential receive pairs	I	
B65	PCIE_RX1-	PCI Express differential receive pairs	I	
B66	WAKE0#	PCI Express wake up signal	I PU	TQ-flexiCFG
B67	WAKE1#	General purpose wake up signal	I PU	TQ-flexiCFG
B68	PCIE_RX0+	PCI Express differential receive pairs	I	
B69	PCIE_RX0-	PCI Express differential receive pairs	I	
B70	GND(FIXED)	Ground	GND	
B71	LVDS_B0+	LVDS Channel B differential pairs 0	O	
B72	LVDS_B0-	LVDS Channel B differential pairs 0	O	
B73	LVDS_B1+	LVDS Channel B differential pairs 1	O	
B74	LVDS_B1-	LVDS Channel B differential pairs 1	O	
B75	LVDS_B2+	LVDS Channel B differential pairs 2	O	
B76	LVDS_B2-	LVDS Channel B differential pairs 2	O	
B77	LVDS_B3+	LVDS Channel B differential pairs 3	O	
B78	LVDS_B3-	LVDS Channel B differential pairs 3	O	
B79	LVDS_BKLT_EN	LVDS / eDP panel backlight enable	O PD	
B80	GND(FIXED)	Ground	GND	
B81	LVDS_B_CK+	LVDS Channel B differential clock	O	
B82	LVDS_B_CK-	LVDS Channel B differential clock	O	
B83	LVDS_BKLT_CTRL	LVDS / eDP panel backlight brightness control	O PD	
B84	VCC_5V_SBY	Standby power input: +5.0V nominal	PWR	
B85	VCC_5V_SBY	Standby power input: +5.0V nominal	PWR	
B86	VCC_5V_SBY	Standby power input: +5.0V nominal	PWR	
B87	VCC_5V_SBY	Standby power input: +5.0V nominal	PWR	
B88	BIOS_DIS1#	Selection straps to determine the BIOS boot device	I PU	
B89	VGA_RED	Red for monitor	O	N/A
B90	GND(FIXED)	Ground	GND	
B91	VGA_GRN	Green for monitor	O	N/A
B92	VGA_BLU	Blue for monitor	O	N/A
B93	VGA_HSYNC	Horizontal sync output to VGA monitor	O	N/A
B94	VGA_VSYNC	Vertical sync output to VGA monitor	O	N/A
B95	VGA_I2C_CK	DDC clock line	O	N/A
B96	VGA_I2C_DAT	DDC data line	IO	N/A
B97	SPI_CS#	Chip select for Carrier Board SPI	O	
B98	(RSVD) SER0_RTS#	Serial port 0 Request To Send	O	TQ-flexiCFG
B99	(RSVD) SER0_CTS#	Serial port 0 Clear To Send	I PU	TQ-flexiCFG
B100	GND(FIXED)	Ground	GND	
B101	FAN_PWMOUT	Fan Pulse Width Modulation speed control output	O	
B102	FAN_TACHIN	Fan tachometer input	I PU	
B103	SLEEP#	Sleep button	I PU	
B104	VCC_12V	Primary wide power input	PWR	
B105	VCC_12V	Primary wide power input	PWR	
B106	VCC_12V	Primary wide power input	PWR	
B107	VCC_12V	Primary wide power input	PWR	
B108	VCC_12V	Primary wide power input	PWR	
B109	VCC_12V	Primary wide power input	PWR	
B110	GND(FIXED)	Ground		

COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
C1	GND(FIXED)	Ground	GND	
C2	GND	Ground	GND	
C3	USB_SSRX0-	SuperSpeed USB3.2 differential receive pairs	I	
C4	USB_SSRX0+	SuperSpeed USB3.2 differentia receive pairs	I	
C5	GND	Ground	GND	
C6	USB_SSRX1-	SuperSpeed USB3.2 differential receive pairs	I	
C7	USB_SSRX1+	SuperSpeed USB3.2 differential receive pairs	I	
C8	GND	Ground	GND	
C9	USB_SSRX2-	SuperSpeed USB3.2 differential receive pairs	I	
C10	USB_SSRX2+	SuperSpeed USB3.2 differential receive pairs	I	
C11	GND(FIXED)	Ground	GND	
C12	USB_SSRX3-	SuperSpeed USB3.2 differential receive pairs	I	
C13	USB_SSRX3+	SuperSpeed USB3.2 differential receive pairs	I	
C14	GND	Ground	GND	
C15	DDI1_PAIR6+	DDI1 DP / HDMI / DVI differential pairs 6	O	N/A
C16	DDI1_PAIR6-	DDI1 DP / HDMI / DVI differential pairs 6	O	N/A
C17	RSVD18	Reserved	NC	
C18	RSVD18	Reserved	NC	
C19	PCIE_RX6+	PCI Express differential receive pairs	I	
C20	PCIE_RX6-	PCI Express differential receive pairs	I	
C21	GND(FIXED)	Ground	GND	
C22	PCIE_RX7+	PCI Express differential receive pairs	I	
C23	PCIE_RX7-	PCI Express differential receive pairs	I	
C24	DDI1_HPD	DDI1 Detection of Hot Plug	I PD	
C25	DDI1_PAIR4+	DDI1 DP / HDMI / DVI differential pairs 4	O	N/A
C26	DDI1_PAIR4-	DDI1 DP / HDMI / DVI differential pairs 4	O	N/A
C27	RSVD18	Reserved	NC	
C28	RSVD18	Reserved	NC	
C29	DDI1_PAIR5+	DDI1 DP / HDMI / DVI differential pairs 5	O	N/A
C30	DDI1_PAIR5-	DDI1 DP / HDMI / DVI differential pairs 5	O	N/A
C31	GND(FIXED)	Ground	GND	
C32	DDI2_CTRLCLK_AUX+	DDI2_CTRLCLK_AUX+ signal DP AUX, HDMI DVI CLK	IO	
C33	DDI2_CTRLDATA_AUX-	DDI2_CTRLDATA_AUX- signal DP AUX, HDMI DVI DATA	IO	
C34	DDI2_DDC_AUX_SEL	Selects the function of DDI2_CTRLxAUX+/- Signals	I PD	
C35	RSVD18	Reserved	NC	
C36	DDI3_CTRLCLK_AUX+	DDI3_CTRLCLK_AUX+ signal DP AUX, HDMI DVI CLK	IO	
C37	DDI3_CTRLDATA_AUX-	DDI3_CTRLDATA_AUX- signal DP AUX, HDMI DVI DATA	IO	
C38	DDI3_DDC_AUX_SEL	Selects the function of DDI3_CTRLxAUX+/- Signals	I PU	
C39	DDI3_PAIR0+	DDI3 DP / HDMI / DVI differential pairs 0	O	
C40	DDI3_PAIR0-	DDI3 DP / HDMI / DVI differential pairs 0	O	
C41	GND(FIXED)	Ground	GND	
C42	DDI3_PAIR1+	DDI3 DP / HDMI / DVI differential pairs 1	O	
C43	DDI3_PAIR1-	DDI3 DP / HDMI / DVI differential pairs 1	O	
C44	DDI3_HPD	DDI3 Detection of Hot Plug	I PD	
C45	RSVD18	Reserved	NC	
C46	DDI3_PAIR2+	DDI3 DP / HDMI / DVI differential pairs 2	O	
C47	DDI3_PAIR2-	DDI3 DP / HDMI / DVI differential pairs 2	O	
C48	RSVD18	Reserved	NC	
C49	DDI3_PAIR3+	DDI3 DP / HDMI / DVI differential pairs 3	O	
C50	DDI3_PAIR3-	DDI3 DP / HDMI / DVI differential pairs 3	O	
C51	GND(FIXED)	Ground	GND	
C52	PEG_RX0+	PCI Express differential receive pairs	I	
C53	PEG_RX0-	PCI Express differential receive pairs	I	
C54	TYPE0#	Type 0 Module indication (NC)	NC	
C55	PEG_RX1+	PCI Express differential receive pairs	I	

COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
C56	PEG_RX1-	PCI Express differential receive pairs	I	
C57	TYPE1#	Type 1 Module indication (NC)	NC	
C58	PEG_RX2+	PCI Express differential receive pairs	I	
C59	PEG_RX2-	PCI Express differential receive pairs	I	
C60	GND(FIXED)	Ground	GND	
C61	PEG_RX3+	PCI Express differential receive pairs	I	
C62	PEG_RX3-	PCI Express differential receive pairs	I	
C63	RSVD18	Reserved	NC	
C64	RSVD18	Reserved	NC	
C65	PEG_RX4+	PCI Express differential receive pairs	I	
C66	PEG_RX4-	PCI Express differential receive pairs	I	
C67	RAPID_SHUTDOWN	Trigger for Rapid Shutdown. Must be driven to 5V	I PD	
C68	PEG_RX5+	PCI Express differential receive pairs	I	
C69	PEG_RX5-	PCI Express differential receive pairs	I	
C70	GND(FIXED)	Ground	GND	
C71	PEG_RX6+	PCI Express differential receive pairs	I	
C72	PEG_RX6-	PCI Express differential receive pairs	I	
C73	GND	Ground	GND	
C74	PEG_RX7+	PCI Express differential receive pairs	I	
C75	PEG_RX7-	PCI Express differential receive pairs	I	
C80	GND(FIXED)	Ground	GND	
C77	RSVD18	Reserved	NC	
C78	PEG_RX8+	PCI Express differential receive pairs	I	
C79	PEG_RX8-	PCI Express differential receive pairs	I	
C80	GND(FIXED)	Ground	GND	
C81	PEG_RX9+	PCI Express differential receive pairs	I	
C82	PEG_RX9-	PCI Express differential receive pairs	I	
C83	RSVD18	Reserved	NC	
C84	GND	Ground	GND	
C85	PEG_RX10+	PCI Express differential receive pairs	I	
C86	PEG_RX10-	PCI Express differential receive pairs	I	
C87	GND	Ground	GND	
C88	PEG_RX11+	PCI Express differential receive pairs	I	
C89	PEG_RX11-	PCI Express differential receive pairs	I	
C90	GND(FIXED)	Ground	GND	
C91	PEG_RX12+	PCI Express differential receive pairs	I	
C92	PEG_RX12-	PCI Express differential receive pairs	I	
C93	GND	Ground	GND	
C94	PEG_RX13+	PCI Express differential receive pairs	I	
C95	PEG_RX13-	PCI Express differential receive pairs	I	
C96	GND	Ground	GND	
C97	RSVD18	Reserved	I/O	TQ-flexiCFG
C98	PEG_RX14+	PCI Express differential receive pairs	I	
C99	PEG_RX14-	PCI Express differential receive pairs	I	
C100	GND(FIXED)	Ground	GND	
C101	PEG_RX15+	PCI Express differential receive pairs	I	
C102	PEG_RX15-	PCI Express differential receive pairs	I	
C103	GND	Ground	GND	
C104	VCC_12V	Primary wide power input	PWR	
C105	VCC_12V	Primary wide power input	PWR	
C106	VCC_12V	Primary wide power input	PWR	
C107	VCC_12V	Primary wide power input	PWR	
C108	VCC_12V	Primary wide power input	PWR	
C109	VCC_12V	Primary wide power input	PWR	
C110	GND(FIXED)	Ground	GND	

COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
D1	GND(FIXED)	Ground	GND	
D2	GND	Ground	GND	
D3	USB_SSTX0-	SuperSpeed USB3.2 differential transmit pairs	O	
D4	USB_SSTX0+	SuperSpeed USB3.2 differential transmit pairs	O	
D5	GND	Ground	GND	
D6	USB_SSTX1-	SuperSpeed USB3.2 differential transmit pairs	O	
D7	USB_SSTX1+	SuperSpeed USB3.2 differential transmit pairs	O	
D8	GND	Ground	GND	
D9	USB_SSTX2-	SuperSpeed USB3.2 differential transmit pairs	O	
D10	USB_SSTX2+	SuperSpeed USB3.2 differential transmit pairs	O	
D11	GND(FIXED)	Ground	GND	
D12	USB_SSTX3-	SuperSpeed USB3.2 differential transmit pairs	O	
D13	USB_SSTX3+	SuperSpeed USB3.2 differential transmit pairs	O	
D14	GND	Ground	GND	
D15	DDI1_CTRLCLK_AUX+	DDI1_CTRLCLK_AUX+ signal DP AUX, HDMI DVI CLK	IO	
D16	DDI1_CTRLDATA_AUX-	DDI1_CTRLDATA_AUX- signal DP AUX, HDMI DVI DATA	IO	
D17	RSVD18	Reserved	NC	
D18	RSVD18	Reserved	NC	
D19	PCIE_TX6+	PCI Express differential transmit pairs	O	
type	PCIE_TX6-	PCI Express differential transmit pairs	O	
D21	GND(FIXED)	Ground	GND	
D22	PCIE_TX7+	PCI Express differential transmit pairs	O	
D23	PCIE_TX7-	PCI Express differential transmit pairs	O	
D24	(RSVD) SER1_RTS#	Serial port 1 Request To Send	O	TQ-flexiCFG
D25	(RSVD) SER1_CTS#	Serial port 1 Clear To Send	I PU	TQ-flexiCFG
D26	DDI1_PAIR0+	DDI1 DP / HDMI / DVI differential pairs 0	O	
D27	DDI1_PAIR0-	DDI1 DP / HDMI / DVI differential pairs 0	O	
D28	RSVD18	Reserved	NC	
D29	DDI1_PAIR1+	DDI1 DP / HDMI / DVI differential pairs 1	O	
D30	DDI1_PAIR1-	DDI1 DP / HDMI / DVI differential pairs 1	O	
D31	GND(FIXED)	Ground	GND	
D32	DDI1_PAIR2+	DDI1 DP / HDMI / DVI differential pairs 2	O	
D33	DDI1_PAIR2-	DDI1 DP / HDMI / DVI differential pairs 2	O	
D34	DDI1_DDC_AUX_SEL	Selects the function of DDI1_CTRLxAUX+/- Signals	I PD	
D35	RSVD18	Reserved	NC	
D36	DDI1_PAIR3+	DDI1 DP / HDMI / DVI differential pairs 3	O	
D37	DDI1_PAIR3-	DDI1 DP / HDMI / DVI differential pairs 3	O	
D38	RSVD18	Reserved	NC	
D39	DDI2_PAIR0+	DDI2 DP / HDMI / DVI differential pairs 0	O	
D40	DDI2_PAIR0-	DDI2 DP / HDMI / DVI differential pairs 0	O	
D41	GND(FIXED)	Ground	GND	
D42	DDI2_PAIR1+	DDI2 DP / HDMI / DVI differential pairs 1	O	
D43	DDI2_PAIR1-	DDI2 DP / HDMI / DVI differential pairs 1	O	
D44	DDI2_HPD	DDI2 Detection of Hot Plug	I PD	
D45	RSVD18	Reserved	NC	
D46	DDI2_PAIR2+	DDI2 DP / HDMI / DVI differential pairs 2	O	
D47	DDI2_PAIR2-	DDI2 DP / HDMI / DVI differential pairs 2	O	
D48	RSVD18	Reserved	NC	
D49	DDI2_PAIR3+	DDI2 DP / HDMI / DVI differential pairs 3	O	
D50	DDI2_PAIR3-	DDI2 DP / HDMI / DVI differential pairs 3	O	
D51	GND(FIXED)	Ground	GND	
D52	PEG_TX0+	PCI Express differential transmit pairs	O	
D53	PEG_TX0-	PCI Express differential transmit pairs	O	
D54	PEG_LANE_RV#	PCI Express Graphics lane reversal input strap	I PU	
D55	PEG_TX1+	PCI Express differential transmit pairs	O	

COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
D56	PEG_TX1-	PCI Express differential transmit pairs	O	
D57	TYPE2#	Type 2 Module indication (GND)	O	
D58	PEG_TX2+	PCI Express differential transmit pairs	O	
D59	PEG_TX2-	PCI Express differential transmit pairs	O	
D60	GND(FIXED)	Ground	GND	
D61	PEG_TX3+	PCI Express differential transmit pairs	O	
D62	PEG_TX3-	PCI Express differential transmit pairs	O	
D63	RSVD18	Reserved	NC	
D64	RSVD18	Reserved	NC	
D65	PEG_TX4+	PCI Express differential transmit pairs	O	
D66	PEG_TX4-	PCI Express differential transmit pairs	O	
D67	GND	Ground	GND	
D68	PEG_TX5+	PCI Express differential transmit pairs	O	
D69	PEG_TX5-	PCI Express differential transmit pairs	O	
D70	GND(FIXED)	Ground	GND	
D71	PEG_TX6+	PCI Express differential transmit pairs	O	
D72	PEG_TX6-	PCI Express differential transmit pairs	O	
D73	GND	Ground	GND	
D74	PEG_TX7+	PCI Express differential transmit pairs	O	
D75	PEG_TX7-	PCI Express differential transmit pairs	O	
D76	GND	Ground	GND	
D77	RSVD18	Reserved	NC	
D78	PEG_TX8+	PCI Express differential transmit pairs	O	
D79	PEG_TX8-	PCI Express differential transmit pairs	O	
D80	GND(FIXED)	Ground	GND	
D81	PEG_TX9+	PCI Express differential transmit pairs	O	
D82	PEG_TX9-	PCI Express differential transmit pairs	O	
D83	RSVD18	Reserved	NC	
D84	GND	Ground	GND	
D85	PEG_TX10+	PCI Express differential transmit pairs	O	
D86	PEG_TX10-	PCI Express differential transmit pairs	O	
D87	GND	Ground	GND	
D88	PEG_TX11+	PCI Express differential transmit pairs	O	
D89	PEG_TX11-	PCI Express differential transmit pairs	O	
D90	GND(FIXED)	Ground	GND	
D91	PEG_TX12+	PCI Express differential transmit pairs	O	
D92	PEG_TX12-	PCI Express differential transmit pairs	O	
D93	GND	Ground	GND	
D94	PEG_TX13+	PCI Express differential transmit pairs	O	
D95	PEG_TX13-	PCI Express differential transmit pairs	O	
D96	GND	Ground	GND	
D97	RSVD18	Reserved	I PU	TQ-flexiCFG
D98	PEG_TX14+	PCI Express differential transmit pairs	O	
D99	PEG_TX14-	PCI Express differential transmit pairs	O	
D100	GND(FIXED)	Ground	GND	
D101	PEG_TX15+	PCI Express differential transmit pairs	O	
D102	PEG_TX15-	PCI Express differential transmit pairs	O	
D103	GND	Ground	GND	
D104	VCC_12V	Primary wide power input	PWR	
D105	VCC_12V	Primary wide power input	PWR	
D106	VCC_12V	Primary wide power input	PWR	
D107	VCC_12V	Primary wide power input	PWR	
D108	VCC_12V	Primary wide power input	PWR	
D109	VCC_12V	Primary wide power input	PWR	
D110	GND(FIXED)	Ground	GND	

4. MECHANICS

4.1 Dimensions

The TQMx110EB has a dimensions of 125 mm × 95 mm (±0.2 mm).
The following figure shows the TQMx110EB three view drawing.

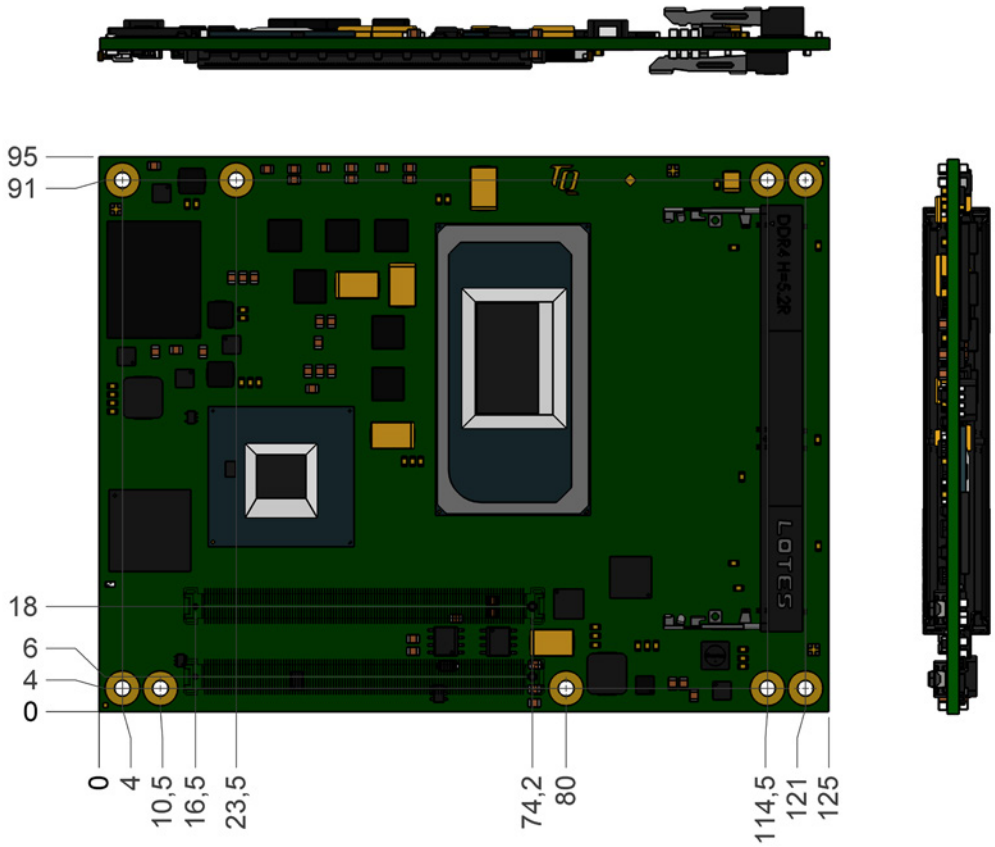


Figure 4: TQMx110EB three view drawing

The following illustration shows the TQMx110EB bottom view.

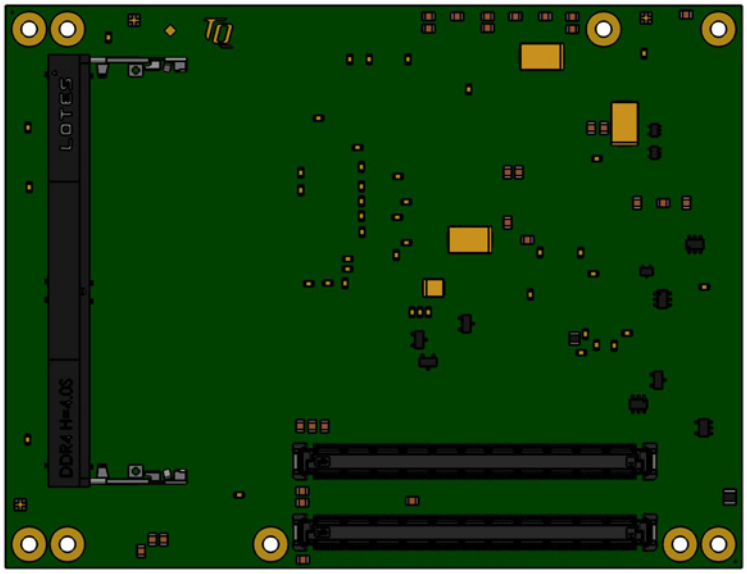


Figure 5: TQMx110EB Bottom View Drawing

4.2 Component Placement

The following illustration shows the TQMx110EB component placement.

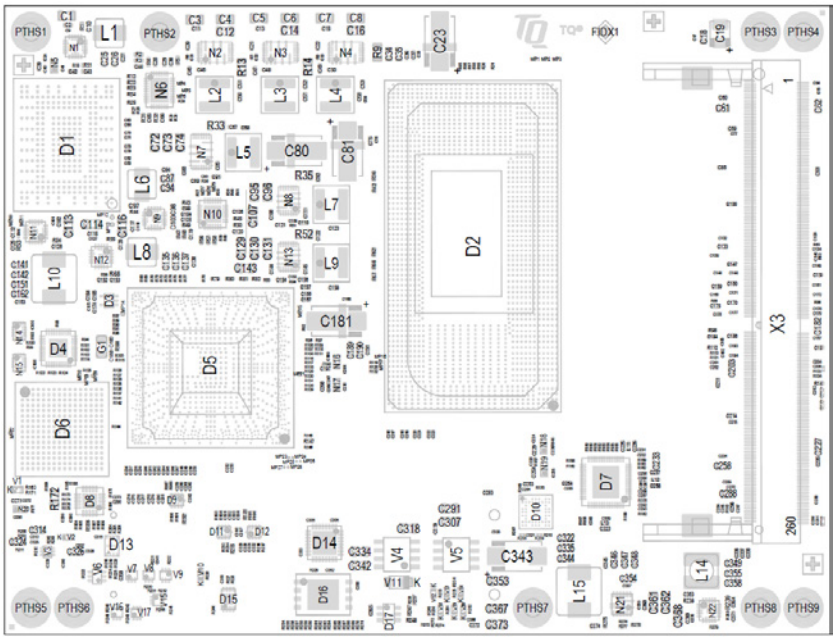


Figure 6: TQMx110EB Component Placement Top

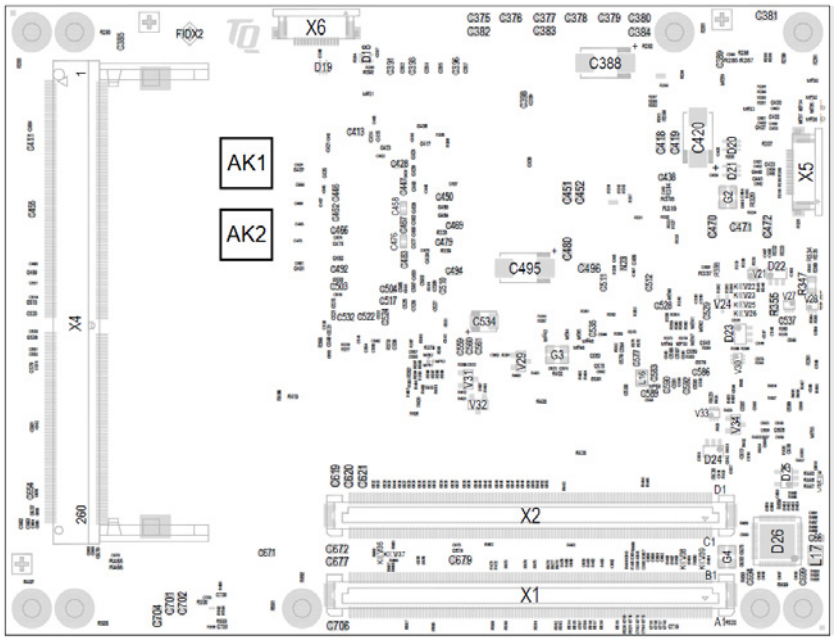


Figure 7: TQMx110EB Component Placement Bottom

The labels on the TQMx110EB show the following information:

Table 18: Labels on TQMx110EB

Label	Text
AK1	MAC address, tests performed
AK2	TQMx110EB version and revision

4.3 Heat Spreader

A heat spreader "TQMx110EB-HSP" is available for the TQMx110EB.
The TQMx110EB is available with or without mounted heat spreader.
The provided heat spreader complies with the latest COM Express™ specification (13 mm ±0.2 mm, including PCB).

The following illustration shows the heat spreader (TQMx110EB-HSP) for the TQMx110EB.

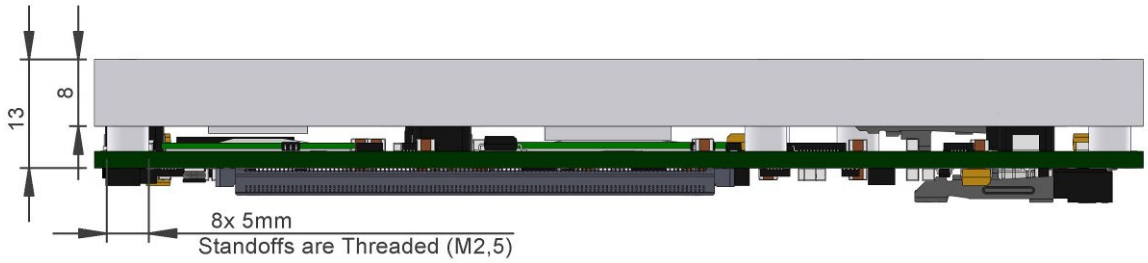


Figure 8: TQMx110EB-HSP Heat Spreader

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.

4.4 Mechanical and Thermal Considerations

The TQMx110EB is designed to operate within a wide range of thermal environments.
An important factor for each system integration is the thermal design. The heat spreader provides the thermal coupling to the TQMx110EB. The heat spreader is thermally coupled to the processor and provides optimal heat transfer from the TQMx110EB to the heat sink. The heat spreader itself is not an appropriate heat sink.
System designers can implement passive and active cooling systems using the thermal connection to the heat spreader.

Attention: Thermal Considerations	
	Do not operate the TQMx110EB without properly attached heat spreader and 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.

4.5 Protection against External Effects

The TQMx110EB itself is not protected against dust, external impact and contact (IP00).
Adequate protection has to be guaranteed by the surrounding system and carrier board.
Conformal coating can be offered for harsh environment applications.

5. SOFTWARE

5.1 System Resources

5.1.1 I²C Bus Devices

The TQMx110EB 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 19: I²C Address Mapping COM Express™ I²C Port

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

5.1.2 SMBus Devices

The TQMx110EB provides a System Management Bus (SMBus).
The following table shows the I²C address mapping for the COM Express™ SMBus port.

Table 20: I²C Address Mapping COM Express™ SMBus Port

8-bit Address	Function	Remark
0xA0, 0xA4	SO-DIMM SPD EEPROMs	Only accessed by the BIOS
0x30, 0x34	SO-DIMM Thermal Sensors	–
0x58	Hardware Monitor	–

5.1.3 Memory Mapping

The TQMx110EB supports the standard PC system memory and I/O memory map.

5.1.4 Interrupt Mapping

The TQMx110EB supports the standard PC Interrupt routing.
The integrated legacy devices (COM1, COM2) can be configured via the BIOS to IRQ3 and IRQ4.

5.2 Operating Systems

5.2.1 Supported Operating Systems

The TQMx110EB supports several Operating Systems:

- Microsoft® Windows® 10 (IoT) Enterprise(64-bit) LTSC RS5 or later
- Linux (i.e. Ubuntu 21.10 or later)

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 TQMx110EB is well supported by the Standard Operating Systems, which already include most of the drivers required.
It is recommended to use the latest Intel® drivers to optimize performance and make use of the full TQMx110EB feature set.

The White Paper "Windows Driver Installation Instructions" provides information how to install the Windows driver.
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 – MENU

The TQMx110EB uses a 64-bit uEFI BIOS.
To access the InsydeH2O BIOS Front Page, the button <ESC> has to be pressed after System Power-Up during POST phase.
If the button is successfully pressed, you will get to the BIOS front page, which shows the main menu items.
For Help Dialog please press <F1>.

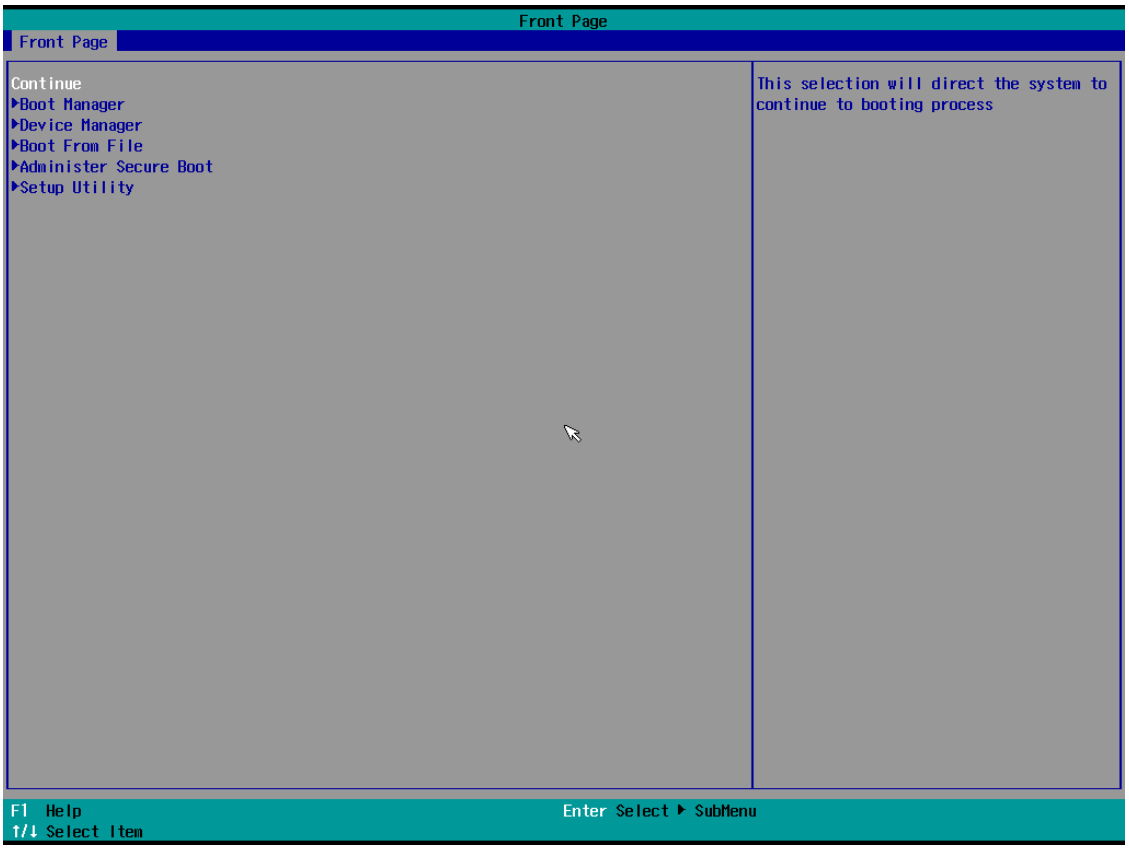


Figure 9: InsydeH2O BIOS Front Page

6.1 Continue

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

6.2 Boot Manager

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

6.3 Device Manager

6.3.1 Driver Health Manager

List all the driver health instances to manage.

6.3.2 Network Device List

Select the network device according the MAC address.

6.4 Boot from File

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

6.5 Administer Secure Boot

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

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

6.6 Setup Utility

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

Key:

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

6.6.1 Main

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

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

6.6.2 Advanced

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

Menu Item	Option	Description
Boot Configuration	See submenu	Configures settings for Boot Phase
SATA Configuration	See submenu	Shows Devices plugged
USB Configuration	See submenu	Configure the USB support
Chipset Configuration	See submenu	Advanced Chipset Configuration options
PCI Subsystem Settings	See submenu	PCI, PCI-X and PCI Express Settings
ACPI Table/Features Control	See submenu	Configures ACPI Tables/Features setting
CPU Configuration	See submenu	CPU Configuration
Power & Performance	See submenu	Power & Performance
Intel® Time Coordinated Computing	See submenu	Intel® Time Coordinated Computing (Intel® TCC) options
Memory Configuration	See submenu	Memory Configuration Parameters
System Agent (SA) Configuration	See submenu	System Agen (SA) Parameters
PCIE Configuration	See submenu	PCIE Parameters
PCH-IO Configuration	See submenu	PCH Parameters
PCH-FW Configuration	See submenu	Configure Management Engine Technology Parameters
ACPI D3Cold Settings	See submenu	ACPI D3Cold related settings
SIO TQMx86	See submenu	Configure CPLD UARTs, TQ Board specific configuration and LVDS
SIO Hardware Monitor Nuvoton NCT7802Y	See submenu	Hardware Monitor and Fan parameters
Console Redirection	See submenu	Configure Console Redirection settings
SIO F81214E	See submenu	Configure UARTs of Fintek Super I/O F81214E

6.6.2.1 Boot Configuration

Setup Utility ⇨ Advanced ⇨ Boot Configuration

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

6.6.2.2 SATA Configuration

Setup Utility ⇨ Advanced ⇨ SATA Configuration

Menu Item	Option	Description
Serial ATA Port X	-	Shows SATA devices plugged

6.6.2.3 USB Configuration

Setup Utility ⇨ Advanced ⇨ USB Configuration

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

6.6.2.4 Chipset Configuration

Setup Utility ⇨ Advanced ⇨ Chipset Configuration

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

6.6.2.5 PCI Subsystem Settings

Setup Utility ⇨ Advanced ⇨ PCI Subsystem Settings

Menu Item	Option	Description
PCI ROM Priority	Legacy ROM / EFI Compatible ROM	In case of multiple Option ROMs (Legacy and EFI Compatible), specifies what PCI Option rom to launch.
External DMA Allowed On Boot	No / Yes	External DMA Allowed On Boot for devices such as 1394, PCMC1A & CardBus.
Install Ext OpRom Before BIOS Setup	Disabled / Ext PCIE Storage OpRom / Ext PCIE Other OpRom / Ex PCIE Both Storage and Other OpRom	Install Ext OpRom for Storage or Other device before BIOS Setup. That we can get the Ext PCIE Card OpRom Setup Menu and have chance to enter into it
PCI Latency Timer	32 PCI Bus Clocks / 64 PCI Bus Clocks / 96 PCI Bus Clocks / 128 PCI Bus Clocks / 160 PCI Bus Clocks / 192 PCI Bus Clocks / 224 PCI Bus Clocks / 248 PCI Bus Clocks	Value to be programmed into PCI Latency Timer Register

6.6.2.6 ACPI Table/Features Control

Setup Utility ⇨ Advanced ⇨ ACPI Table/Features Control

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

Setup Utility ⇨ Advanced ⇨ RC Advanced Menu ⇨ ACPI Settings

Menu Item	Option	Description
Enable ACPI Auto Configuration	[ ] / [X]	Enables or disables BIOS ACPI auto configuration
Enable Hibernation	[ ] / [X]	Enables or disables system ability to hibernate (OS/S4 Sleep State). This option may not be effective with some OSs.
PTID Support	[ ] / [X]	PTID support will be loaded if enabled.
PECI Access Method	Direct I/O / ACPI	PECI access method is Direct I/O or ACPI.
ACPI S3 support	Enabled / Disabled	Enable ACPI S3 support.
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
ACPI Debug	Enabled / Disabled	Open a memory buffer for storing debug strings. Reenter SETUP after enabling to see the buffer address. Use method ADBG to write strings to buffer.
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.

6.6.2.7 CPU Configuration

Setup Utility ⇨ Advanced ⇨ CPU Configuration

Menu Item	Options	Description
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.
PECI	Enabled / Disabled	Enable/Disable PECI.
AVX	Enabled / Disabled	Enable/Disable AVX 2/3 Instruxtions.
AVX3	Enabled / Disabled	Enable/disable AVX 3 Instructions.
Active Processor Cores	All / 1 / 2 / 3	Number of cores to enable in each processor package.

Menu Item	Options	Description
Hyper-Threading	Enabled / Disabled	Enable or Disable Hyper-Threading Technology.
BIST	Enabled / Disabled	Enable or Disable BIST (Built-In Self-Test) on reset.
AES	Enabled / Disabled	Enable or Disable AES (Advanced Encryption Standard).
MachineCheck	Enabled / Disabled	Enable or Disable Machine Check.
MonitorMWait	Enabled / Disabled	Enable or Disable MonitorMWait.

6.6.2.8 Power & Performance

Setup Utility ⇨ Advanced ⇨ Power & Performance

Menu Item	Options	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 ⇨ Power & Performance ⇨ CPU – Power Management Control

Menu Item	Options	Description
Boot performance mode	Max Battery / Max Non-Turbo Performance / Turbo Performance	Select the performance state that the BIOS will set starting from reset vector.
Intel® SpeedStep™	Enabled / Disabled	Allows more than two frequency ranges to be supported.
Race To Halt (RTH)	Enabled / Disabled	Enable or Disable Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)
Intel® Speed Shift Technology	Enabled / Disabled	Enable or Disable Intel® Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.
Intel® Speed Shift Technology Interrupt Control	Enabled / Disabled	Enable/Disable Intel® Speed Shift Technology Interrupts
Intel® Turbo Boost Max Technology 3.0	Enabled / Disabled	Enable/Disable Intel® Trubo Boost Max Technology 3.0 support. Disabling will report the maximum ratio of the slowest core in _CPC object.
Per Core P State OS control mode	Enabled / Disabled	Enable/Disable Per Core P state OS control mode. Disabling will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core requests.
HwP Autonomous Per Core P State	Enabled / Disabled	Disable Autonomous PCPS (Bit 30 = 1, command 0x11) Autonomous will request the same value for all cores all the time. Enable PCPS (default Bit 30 = 0, command 0x11)
HwP Autonomous EPP Grouping	Enabled / Disabled	Enable EPP grouping (default Bit 29 = 0, command 0x11) Autonomous will request the same values for all cores with same ePP. Disable EPP grouping (Bit 29 = 1, command 0x11) autonomous will not necessarily request same values for all cores with same EPP.
HwP Fast MSR Support	Enabled / Disabled	Enable/Disable HwP Fast MSR Support for IA32_HWP_REQUEST MSR.
HDC Control	Enabled / Disabled	This option allows HDC configuration. Disabled: Disable HDC Enabled: Can be enabled by OS if OS native support is available.
Turbo Mode	Enabled / Disabled	Enable or Disable processor Turbo Mode (requires Intel® Speed Step or Intel® Speed Shift to be available and enabled).
View/Configure Turbo Options	See submenu	Configure Turbo Options.

Menu Item	Options	Description
Config TDP Configurations	See submenu	Configure TDP Options.
Platform PL1 Enable	Enabled / Disabled	Enable/Disable Platform Power Limit 1 programming. If this option is enabled. It activates the PL1 value to be used by the processor to limit the average power of given time window.
Platform PL2 Enable	Enabled / Disabled	Enable/Disable Platform Power Limit 2 programming. If this option is disabled, BIOS will program the default values for Platform Power Limit 2.
Power Limit 3 Settings	See submenu	Power Limit 3 Settings.
Power Limit 4 Override	Enabled / Disabled	Enable/Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Power Limit 4.
C states	Enabled / Disabled	Enable or Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
C-State Auto Demotion	Disabled / C1 / C3 / C1 and C3	Configure C-State Auto Demotion. This option will be hidden if C states is Disabled.
C-State Un-demotion	Disabled / C1 / C3 / C1 and C3	Configure C-State Un-demotion. This option will be hidden if C states is Disabled.
Package C-State Demotion	Enabled / Disabled	Package C-State Demotion. This option will be hidden if C states is Disabled.
Package C-State Un-demotion	Enabled / Disabled	Package C-State Un-demotion. This option will be hidden if C states is Disabled.
CState Pre-Wake	Enabled / Disabled	Disabled: Sets bit 30 of Power_CTL MSR (0x1FC) to 1 to disable the CState Pre-Wake. This option will be hidden if C states is Disabled.
IO MWAIT Redirection	Enabled / Disabled	When set, will map IO_read intstructions sent to IO registers PMG_IO_BASE_ADDRBASE + offset to MWAIT(offset)
Package C State Limit	C0/C1 / C2 / C3 / C6 / C7 / C7S / C8 / C9 / C10 / CPU Default / Auto	Maximum Package C State Limit Setting. CPU Default: Leaves to Factory default value. Auto: Initializes to deepest available Package C State Limit. This option will be hidden if C states is Disabled.
Thermal Monitor	Enabled / Disabled	Enable or Disable Thermal Monitor. This option will be hidden if C states is Disabled.
Interrupt Redirection Mode Selection	Fixed Priority / Round robin / Hash Vector / No Change	Interrupt Redirection Mode Select for Logical Interrupts.
Timed MWAIT	Enabled / Disabled	Enable/Disable Timed MWAIT Support.
CPU Lock Configuration	See submenu	CPU Lock Configuration.

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

Menu Item	Options	Description
Energy Efficient P-state	Enabled / Disabled	Enable/Disable Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 ECX[3] will read 0 indicating no support for Energy Efficient policy setting. When set to 1 will enable access to ENERGY_PERFORMANCE_BIAS MSR 1B0h and CPUID Function 6 ECX[3] will read 1 indicating Energy Efficient policy setting is supported.
Package Power Limit MSR Lock	Enabled / Disabled	Enable/Disable locking of Package Power Limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will

Menu Item	Options	Description
		be required to unlock the register.
X-Core Turbo Ratio Limit Ratio (TRLR) override	[X]	X-Core Turbo Ratio Limit Ratio (TRLR) with range of Max Non-Turbo Ratio up to 120.
Energy Efficient Turbo	Enabled / Disabled	Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overclocking situations where turbo frequency must remain constant. Otherwise, leave enabled.

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

Menu Item	Options	Description
Enable Configurable TDP	Applies to non-cTDP / Applies to cTDP	Applies TDP initialization settings basen on non-cTDP or cTDP. Default is 1: Applies to cTDP; if 0 then applies to non cTDP and BIOS will bypass cTDP initialization flow.
Configurable TDP Boot Mode	Nominal / Down / Up / Deactivate	Configurable TDP Mode as Nominal/Up/Down/Deactivate TDP selection. Deactivate option will set MSR to Nominal and MMIo to Zero.
Configurable TDP Lock	Enabled / Disabled	Configurable TDP Mode Lock sets the Lock bits on TURBO_ACTIVATION_RATIO and CONFIG_TDP_CONTROL. Note: When CTDP Lock is enabled Custom ConfigTDP Count will be forced to 1 and Custom ConfigTDP Boot index will be forced to 0.
Power Limit 1	0 – X	Power Limit 1 in milliwatts. 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.
Power Limit 2	0 – X	Power Limit 2 value in milliwatts. BIOS will round to the nearest 1/8 W when programming. 0 = no custom override. For 12.50 W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window	0 – 128	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = use default value (28 sec). Defines time window which TDP value should be maintained.
ConfigTDP Turbo Activation Ratio	0 – 125	Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don't use custom value.

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

Menu Item	Options	Description
Power Limit 3 Override	Enabled / Disabled	Enable/Disable Power Limit 3 override. If this option is disabled, BIOS will leave the hardware default values for Power Limit 3 and Power limit 3 Time Window.
Power Limit 3	[X]	Power Limit 3 in Milli Watts. BIOS will round to the nearest 1/8W when programming. For 12.5W, enter 12500. XE SKU: Any value can be programmed. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP Limit. If value is 0, BIOS leaves the hardware default value.
Power Limit 3 Time Window	[X]	Power Limit 3 Time Window value in Milli seconds. The value may vary from 3 to 64(max). Indicates the time window over which Power Limit 3 value should be maintained. If the value is 0, BIOS leaves the hardware default value.

Menu Item	Options	Description
Power Limit 3 Duty Cycle	[X]	Specify the duty cycle in percentage that the CPU is required to maintain over the configured time window. Range is 0-100
Power Limit 3 Lock	Enabled / Disabled	Power Limit 3 MSR 615h Lock. When enabled PL3 configurations are locked during OS. When disabled PL3 configuration can be changed during OS.

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

Menu Item	Options	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 ⇨ Power & Performance ⇨ GT – Power Management Control

Menu Item	Options	Description
RC6 (Render Standby)	Enabled / Disabled	Check to enable render standby support.
Maximum GT frequency	Default Max Frequency / 100 – 1200 MHz	Maximum GT frequency limited by the user. Choose between 300 MHz (RPM) and 1150 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.

6.6.2.9 Intel® Time Coordinated Computing

Setup Utility ⇨ Advanced ⇨ Intel® Time Coordinated Computing

Menu Item	Options	Description
#AC Split Lock	Enabled / Disabled	Enable or Disable Alignment Check Exception (#AC). When enabled, this will assert an #AC when any atomic operation has an operand that crosses two cache lines.
IFU Enable	Enabled / Disabled	Enable or Disable Instruction Fetch Unit (IFU). When enabled, Instructions will be prefetch to the cache.
Intel® TCC Authentication	OEM Enrolled Key	Intel® TCC Authentication determines the key to be used. OEM Enrolled Key is built in by OEM. Non-OEM Enrolled Key can be add by user.
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!
OPIO Recentering	Enabled / Disabled	Enable or Disable Opio Recentering to improve Pcie latency.

6.6.2.10 Memory Configuration

Setup Utility ⇨ Advanced ⇨ 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

6.6.2.11 System Agent (SA) Configuration

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration

Menu Item	Options	Description
Graphics Configuration	See submenu	Configure some graphical options.
DMI/OPI Configuration	See submenu	Control various DMI functions.
VMD setup menu	See submenu	VMD Configuration settings
PCI Express Configuration	See submenu	PCI Express Configuration settings.
Stop Grant Configuration	Auto / Manual	Automatic/Manual stop grant configuration
VT-d	Enabled / Disabled	VT-d capability.
X2APIC Opt Out	Enabled / Disabled	Enable or Disable X2APIC_OPT_OUT bit.
DMA Control Guarantee	Enabled / Disabled	Enable or Disable DMA_CONTROL_GUARANTEE bit.
Thermal Device (B0:D4:F0)	Enabled / Disabled	Enable or Disable SA Thermal Device.
Cpu CrashLog (Device 10)	Enabled / Disabled	Enable or Disable Cpu CrashLog Device.
GNA Device (B0:D8:F0)	Enabled / Disabled	Enable or Disable SA GNA Device.
CRID Support	Enabled / Disabled	Enable or Disable CRID control for Intel SIPP.
WRC Feature	Enabled / Disabled	Enable or Disable SA WRC (Write Cache) Feature of IOP. When enabled, supports IO devices allocating onto the ring and into LLC.
VCRt mapping to PEG	Enabled / Disabled	Enable or Disable VCRt mapping to PEG. When enabled, VCRt mapping to PEG.
Above 4 GB MMIO BIOS assignment	Enabled / Disabled	Enable or Disable above 4 GB MemoryMappedIO BIOS assignment. This is enabled automatically when Aperture Size is set to 2048 MB.
IPU Device (B0:D5:F0)	Enabled / Disabled	Enable or Disable SA IPU Device.

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

Menu Item	Option	Description
Graphics Turbo IMON Current	[X]	Graphics turbo IMON current values supported (14 – 31)
Skip Scanning of External Gfx Card	Enabled / Disabled	If enabled, it will not scan for External Gfx Card on PEG and PCH PCIE Ports.
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.

Menu Item	Option	Description
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.
DFD Restore	Enabled / Disabled	Select Display memory map programming for DFD Restore.
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.
Configure GT for use	Enabled / Disabled	Enable/Disable GT configuration in BIOS.
RC1p Support	Enabled / Disabled	Enable/Disable RC1p support. If RC1p is enabled, send a RC1p frequency request to PMA based other conditions being met.
PAVP Enable	Enabled / Disabled	Enable/Disable PAVP.
Cdynmax Clamping Enable	Enabled / Disabled	Enable/Disable Cdynmax Clamping.
Cd Clock Frequency	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.
IUER Button Enable	Enabled / Disabled	Enable/Disable IUER Button Functionality.
LCD Control	See submenu	LCD Control options.

Setup Utility ⇨ Advanced ⇨ 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.
Active LFP	No eDP / eDP Port-A	Select the Active LFP configuration.
Panel Color Depth	18 Bit / 24 Bit	Select the LFP Panel Color Depth
Backlight Brightness	[X]	Sel VBIOS Brightness.

Menu Item	Option	Description
		Range: 0-255

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration ⇨ DMI/OPI Configuration

Menu Item	Option	Description
DMI Gen3 ASPM	Disabled / Auto / ASPM L0s / ASPM L2 / ASPM L0sL1	GMI Gen3 ASPM Support
DMI Gen3 ASPM Control	Disabled / Auto / ASPM L0s / ASPM L2 / ASPM L0sL1	DMI Gen3 ASPM Control Support.
DMI Gen3 L1 Exit Latency	[X]	DMI Gen3 L1 Exit Latency.

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

Menu Item	Option	Description
Enable VMD Controller	Enabled / Disabled	Enable/Disable VMD Controller. When enabled VMD options were unhided.
Enable VMD Global Mapping	Enabled / Disabled	Enable/Disable VMD Global Mapping.
Map this Root Port under VMD	Enabled / Disabled	Map/UnMap this Root Port to VMD
Raid 0	Enabled / Disabled	Enable/Disable RAID0 support.
Raid 1	Enabled / Disabled	Enable/Disable RAID1 support.
Raid 5	Enabled / Disabled	Enable/Disable RAID5 support.
Raid 10	Enabled / Disabled	Enable/Disable RAID10 support.
Intel Rapid Recovery Technology	Enabled / Disabled	Enable/Disable Intel Rapid Recovery Technology.
RRT volumes can span internal and eSATA drivers	Enabled / Disabled	Enable/Disable RRT volumes can span internal and eSATA drivers.
Intel® Optane™ Memory	Enabled / Disabled	Enable/Disable System Acceleration with Intel® Optane™ Memory feature.

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

Menu Item	Option	Description
PCI Express Clock Gating	Enabled / Disabled	PCI Express Clock Gating Enable/Disable for each root port.
Fia Programming	Enabled / Disabled	Load Fia Configuration if Enabled for each root port.
PCI Express Power Gating	Enabled / Disabled	PCI Express Power Gating Enable/Disable for each root port.
Compliance Test Mode	Enabled / Disabled	Enable when using Compliance Load Board.
PCIe function swap	Enabled / Disabled	When Disabled, prevents PCIE root port function swap. If any function other than 0^{th} is enabled, 0^{th} will become visible.
CDR Relock for PEG60	Enabled / Disabled	Enable/Disable CDR Relock.
NewFOM for PEG60	Enabled / Disabled	Enable/Disable New FOM
CDR Relock for PEG10	Enabled / Disabled	Enable/Disable CDR Relock.
NewFOM for PEG10	Enabled / Disabled	Enable/Disable New FOM

Menu Item	Option	Description
PCIE Resizable BAR Support	Enabled / Disabled	Enable/Disable PCIE Resizable BAR Support.
PCI Express Root Port X	See submenu	PCI Express Root Port Settings. Port 1 – onboard SSD. Port2, 3, 4 – PEG Port

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration ⇨ PCI Express Configuration ⇨ PCI Express Root Port X

Menu Item	Options	Description
PCI Express Root Port X	Enabled / Disabled	Control the PCI Express root port.
Connection Type	Built-in / Slot	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
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.
Gen3 Eq Phase3 Method	Hardware / Static Coeff.	PCIe Gen3 Equalization Phase 3 Method.
Gen4 Eq Phase3 Method	Hardware / Static Coeff.	PCIe Gen4 Equalization Phase 3 Method.
ACS	Enabled / Disabled	Enable or Disable Access Control Services extended capability.
PTM	Enabled / Disabled	Enable or Disable Precision Time Measurement.
DPC	Enabled / Disabled	Enable or Disable Downstream Port Containment.
FOM Scoreboard Control Policy	Auto / Gen3 / Gen4 / Gen3/Gen4	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
VC	Enabled / Disabled	Enable/Disable Virtual Channel
Multi-VC	Enabled / Disabled	Enable/Disable Multi Virtual Channel.
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.
CT0	Enabled / Disabled	PCI Express Completion Timer T0 Enable/Disable.
SEFE	Enabled / Disabled	Root PCI Express System Error on Fatal Error enable/disable.
SENFE	Enabled / Disabled	Root PCI Express System Error on Non-Fatal Error enable/disable.
SECE	Enabled / Disabled	Root PCI Express System Error on Correctable Error enable/disable.
PME SCI	Enabled / Disabled	PCI Express PME SCI enable/disable.
Hot Plug	Enabled / Disabled	PCI Express Hot Plug enable/disable.
Advanced Error Reporting	Enabled / Disabled	Advanced Error Reporting enable/disable.
PCIe Speed	Auto / Gen1 / Gen2 / Gen3	Configure PCIe Speed.
IOTG Mode	Enabled / Disabled	IOTG Mode Enable/Disable
Transmitter Half Swing	Enabled / Disabled	Transmitter Half Swing enable/disable.
Detect Timeout	[X]	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
P2P Support	Enabled / Disabled	Program P2P Support Registers according to setup option.
LTR	Enabled / Disabled	PCH PCIE Latency Reporting enable/disable.
Snoop Latency Override	Auto / Manual / Disabled	Snoop Latency Override for PCH PCIE. Disabled: Disable override

Menu Item	Options	Description
		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.
UPTP	[X]	Upstream Port Transmitter Preset.
DPTP	[X]	Downstream Port Transmitter Preset

6.6.2.12 PCIE Configuration

Setup Utility ⇨ Advanced ⇨ PCIE Configuration ⇨ IMR Configuration

Menu Item	Options	Description
PCIe IMR	Enabled / Disabled	Enable/Disable PCIe IMR
PCIe IMR Size	[X]	PCIe Reserved Memory Size to be requested in MB. Maximum value of 1024 MB.
PCIe RP Location for IMR	PCH PCIE / SA PCIE	Select SA or PCH root port associated with IMR.
RP Index for IMR	[X]	Selects which root port will be associated with IMR.

6.6.2.13 PCH-IO Configuration

Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration

Menu Item	Options	Description
PCI Express Configuration	See submenu	PCI Express Configuration settings.
SATA And RST Configuration	See submenu	SATA Device Options settings.
USB Configuration	See submenu	USB Configuration settings.
HD Audio Configuration	See submenu	HD Audio Subsystem Configuration Settings.
PXE ROM	Enabled / Disabled	Enable or Disable PXE Option ROM execution.
State After G3	S0 State / S5 State	Specify what state to go to when power is re-applied after a power failure (G3 state).
Compatible Revision ID	Enabled / Disabled	Enable/Disable Compatible Revision ID
Enable TCO Timer	Enabled / Disabled	Enable/Disable TCO timer. When disabled, it disables PCH ACPI timer, stops TCO timer, and ACPI WDAT table will not be published
Enable Timed GPIO0	Enabled / Disabled	Enable/Disable timed GPIO0. When disabled, it disables cross time slamp time synchronization as extension of Hammock Harbor time synchronization.
Enable Timed GPIO1	Enabled / Disabled	Enable/Disable timed GPIO1. When disabled, it disables cross time slamp time synchronization as extension of Hammock Harbor time synchronization.
Pcie Pll SSC	Auto / X% / Disable	Pcie Pll SSC percentage. Auto – Keep HW default, no BIOS override Range is 0.0% - 2.0%

Menu Item	Options	Description
Enable 8254 Clock Gate	Enabled / Disabled	Enable/Disable 8254 glock gate in early phase. Set 8254CGE is necessary for SLP_S0 support. Platform is able to disable this policy and set 8254CGE in late phase.
Lock PCH Sideband Access	Enabled / Disabled	Lock PCH Sideband access, include SideBand interface lock and SideBand PortID mask for certain end point (e.g. PSFx). The option is invalid if POSTBOOT SAL is set.
Flash Protection Range Registers (FPRR)	Enabled / Disabled	Enable Flash Protection Range Registers.
SPD Write Disable	True / False	Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.
LGMR	Enabled / Disabled	64KB memory block for LGMR (LPC Memory Range Decode)
OS IDLE Mode	Enabled / Disabled	Enable/Disable OS idle Mode Feature.

PCI Express Configuration

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

Menu Item	Option	Description
DMI Link ASPM Control	Disabled / L0s / L1 / L0xL1 / Auto	The control of Active State Power Management of the DMI Link.
Peer Memory Write Enable	Enabled / Disabled	Peer Memory Write Enable/Disable.
Compliance Test Mode	Enabled / Disabled	Enable when using Compliance Load Board.
PCIe function swap	Enabled / Disabled	When disabled, prevents PCIE rootport function swap. If any function other than 0^{th} is enabled, 0^{th} will become visible.
PCIe EQ settings	See submenu	This form contains options for controlling PCIe EQ process.
PCI Express Root Port X	See submenu	Configuration of the corresponding PCI Express Root Port X.

Setup Utility ⇨ Advanced ⇨ 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
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 ⇨ PCH-IO Configuration ⇨ PCI Express Configuration ⇨ PCI Express Root Port X

Menu Item	Options	Description
PCI Express Root Port X	Enabled / Disabled	Control the PCI Express root port.
Connection Type	Built-in / Slot	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
ASPM	Disabled / L0s / L1 / L0sL1 / Auto	PCI Express Active State Power Management settings.
L1 Substates	Disabled / L1.1 / L1.1 & L1.2	PCI Express L1 Substates settings.
ACS	Enabled / Disabled	Enable or Disable Access Control Services extended capability.
PTM	Enabled / Disabled	Enable or Disable Precision Time Measurement.
DPC	Enabled / Disabled	Enable or Disable Downstream Port Containment.
EDPC	Enabled / Disabled	Enable or Disable Rootport extensions for Downstream Port Containment.
URR	Enabled / Disabled	PCI Express Unsupported Request Reporting enable/disable.
FER	Enabled / Disabled	PCI Express Device Fatal Error Reporting enable/disable.
NFER	Enabled / Disabled	PCI Express Device Non-Fatal Error Reporting enable/disable.
CER	Enabled / Disabled	PCI Express Device Correctable Error Reporting enable/disable.
SEFE	Enabled / Disabled	Root PCI Express System Error on Fatal Error enable/disable.
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.
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.

SATA And RST Configuration

Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ SATA And RST 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 Test Mode	Enabled / Disabled	Test Mode enable/disable (Loop Back).
Software Feature Mask Configuration	See submenu	RST Legacy OROM/RST UEFI driver will refer to the SWFM configuration to enable/disable the storage features.
Aggressive LPM Support	Enabled / Disabled	Enable PCH to aggressively enter link power state.
Serial ATA Port X	Enabled / Disabled	Enable or Disable SATA Port.
Hot Plug	Enabled / Disabled	Designates this port as Hot Pluggable.
External	Enabled / Disabled	Marks this port as external.
Spin Up Device	Enabled / Disabled	If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive /	Identify the SATA port is connected to Solid State Drive or Hard Disk

Menu Item	Options	Description
	Solid State Drive	Drive.
Topology	Unknown / ISATA / Direct Connect / Flex / M2	Identify the SATA topology if it is Default or ISATA or Flex or DirectConnect or M2.
SATA Port X DevSlp	Enabled / Disabled	Enable/Disable SATA Port 0 DevSlp. For DevSlp to work, both hard drive and SATA port need to support DevSlp function, otherwise an unexpected behaviour might happen. Please check board design before enabling it.
DITO Configuration	Enabled / Disabled	Enable or Disable DITO configuration.
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.

USB Configuration

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

Menu Item	Options	Description
xDCI Support	Enabled / Disabled	Enable/Disable xDCI (USB OTG Device)
USB PD0 Programming	Enabled / Disabled	Select 'Enabled' if Port Disable Override functionality is used.
XHCI LTR Mode	Enabled / Disabled	Enable/Disable XHCI LTR Mode.
USB Overcurrent	Enabled / Disabled	Select 'Disabled' for pin-based debug. If pin based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.
USB Overcurrent Lock	Enabled / Disabled	Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data.
USB Port Disable Override	Select per Pin / Disabled	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.
USB SS/HS Physical Connector #X	Enabled / Disabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.

Security Configuration

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

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

HDA Audio Configuration

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

Menu Item	Options	Description
HD Audio	Enabled / Disabled	Control detection of the HD-Audio device. Disabled: HAD will be unconditionally disabled. Enabled: HAD will be unconditionally enabled.
Audio DSP	Enabled / Disabled	Enable or disable Audio DSP.
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.

6.6.2.14 PCH-FW Configuration

Setup Utility ⇨ Advanced ⇨ PCH-FW Configuration

Menu Item	Option	Description
ME State	Enabled / Disabled	When Disabled ME will be put into ME Temporarily Disabled Mode.
Firmware Update Configuration	See submenu	Configure Management Engine Technology parameters.
Extend CSME Measurement to TPM-PCR	Enabled / Disabled	Enable/Disable Extend CSME Measurement to TPM-PCR[0] and AMT Config to TPM-PCR[1]

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

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

6.6.2.15 ACPI D3Cold settings

Setup Utility ⇨ Advanced ⇨ ACPI D3Cold settings

Menu Item	Option	Description
ACPI D3 Cold Support	Enabled / Disabled	Enable/Disable ACPI D3Cold support to be executed on D3 entry and exit.
VR Ramp up delay	[X]	Delay between subsequent VR ramp ups if they are all turn ON at the same time.
PCIE Slot 5 Device Power-on delay in ms	[X]	Delay between applying core power and Deasserting PERST#.
Audio Delay	[X]	Delay after applying power to HD Audio (Realtek) codec device.
SensorHub	[X]	Delay after applying power to SensorHub device.
TouchPad	[X]	Delay after applying power to TouchPad device.
TouchPanel	[X]	Delay after applying power to TouchPanel device.
P-state capping	Enabled / Disabled	Set _PPC and send ACPI notification.
USB Port 1	High Speed / Super Speed / Disabled	USB RTD3 support. Super Speed: USB3.0 devices will be exposed as RTD3 capable. High Speed: USB2.0 devices will be exposed as RTD3 capable. Disabled: USB RTD3 support disabled.

Menu Item	Option	Description
USB Port 2	High Speed / Super Speed / Disabled	USB RTD3 support. Super Speed: USB3.0 devices will be exposed as RTD3 capable. High Speed: USB2.0 devices will be exposed as RTD3 capable. Disabled: USB RTD3 support disabled.
ZPODD	Enabled / Disabled	Zero Power ODD option is applicable only for the board with ZPODD support.
Bluetooth	Enabled / Disabled	Enable/Disable RTD3 support for BT.
Sata Port 0	Enabled / Disabled	Setup option to control the SATA port RTD3 functionality.
Sata Port 1	Enabled / Disabled	Setup option to control the SATA port RTD3 functionality.
Sata Port 2	Enabled / Disabled	Setup option to control the SATA port RTD3 functionality.
Sata Port 3	Enabled / Disabled	Setup option to control the SATA port RTD3 functionality.
Sata Port 4	Enabled / Disabled	Setup option to control the SATA port RTD3 functionality.
Sata Port 5	Enabled / Disabled	Setup option to control the SATA port RTD3 functionality.
PCIe Remapped CR1	Enabled / Disabled	PCIe RTD3 setup conflicts with SATA RTD3. Platform specific.
PCIe Remapped CR2	Enabled / Disabled	PCIe RTD3 setup conflicts with SATA RTD3. Platform specific.
PCIe Remapped CR3	Enabled / Disabled	PCIe RTD3 setup conflicts with SATA RTD3. Platform specific.

6.6.2.16 SIO TQMx86

Setup Utility ⇨ Advanced ⇨ SIO TQMx86

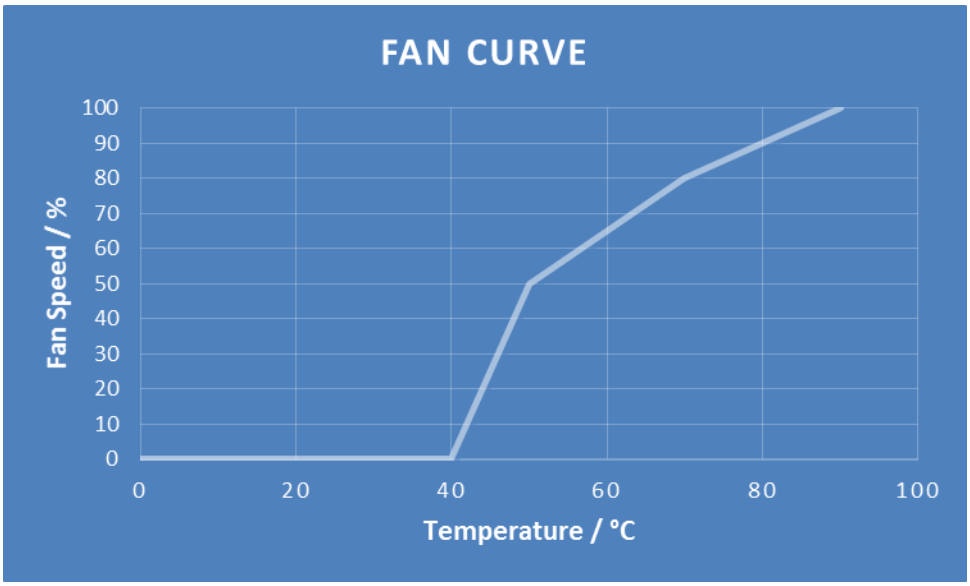
Menu Item	Option	Description
Serial Port X	Enabled / Disabled / Auto	Disabled: No configuration Enabled: User Configuration Auto: EFI/OS chooses configuration
Base I/O Address	2E8 / 2F8 / 3E8 / 3F8	Configure Base I/O Address of corresponding Serial Port X.
Interrupt	IRQ3 / IRQ4 / IRQ5 / IRQ6 / IRQ7	Configure 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 / 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.
PEG PCI Express Configuration	1x16 / 2x8 / 2x4, 1x8	Configure different PEG PCI Express Configurations. Note: A cold reset is required to assume this configuration.
COM Express eDP/LVDS Configuration	LVDS / eDP	Configure if eDP or LVDS is connected to the COM Express Connector.
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 % /	Configure LVDS clock frequency center spreading depth.

Menu Item	Option	Description
	2.0 % / 2.5 %	
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.

6.6.2.17 SIO Hardware Monitor Nuvoton NCT7802Y

Setup Utility ⇨ Advanced ⇨ SIO Hardware Monitor Nuvoton NCT7802Y

Menu Item	Options	Description
Hardware Monitor	See submenu	Set Hardware Monitor parameters.
Fan PWM Frequency	Low (32 Hz) / High (25 kHz)	Select PWM Frequency for the FAN.
Enable Fan Scaling	[ ] / [X]	Enabling Fan Scaling unhides a menu to define trip points to configure the Fan Speed / Temperature curve. The default is shown in the diagram below.



6.6.2.18 Console Redirection

Setup Utility ⇨ Advanced ⇨ Console Redirection

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

If enabled:

Menu Item	Options	Description
Terminal Type	VT_100 / VT_100+ / VT_UTF8 / PC_ANSI	Select the Console Redirection terminal type.
Baud Rate	115200 / 57600 / 38400 / 19200 / 9600 / 4800 / 2400 / 1200	Select the Console Redirection Baud Rate.
Data Bits	7 Bits / 8 Bits	Select the Console Redirection Data Bits.
Parity	None / Even / Odd	Select the Console Redirection Parity Bits.
Stop Bits	1 Bit / 2 Bits	Select the Console Redirection Stop Bits.
Flow Control	None / RTS/CTS / XON/XOFF	Select the Console Redirection Flow Control type.
Information Wait Time	0 Second / 2 Second / 5 Second / 10 Second / 30 Second	Select the Console Redirection Port information display time.
C.R. After Legacy Boot	Yes / No	Console Redirection continue works after Legacy Boot.
Text Mode Resolution	AUTO / Force 80×25 / Force 80×24 (DEL FIRST ROW) / Force 80×24 (DEL LAST ROW)	Console Redirection Text Mode Resolution. Auto: Follow VGA text mode Force 80×25: Don't care about VGA and force text mode to be 80×25 Force 80×24 (DEL FIRST ROW): Don't care about VGA and force text mode to be 80×24 and Del first row Force 80×24 (DEL LAST ROW): Don't care about VGA and force text mode to be 80×24 and Del last row
Auto Refresh	Enabled / Disabled	When feature enable, screen will be auto refresh once after detect remote terminal was connected.
Auto adjust Terminal resolution	Enabled / Disabled	Through send extra ESC sequence code
COM_X	See submenu	Set parameters of COM Express Serial Port X. Whereby X stands for COM Express Serial Port 0 (Insyde name COMA) or 1 (Insyde name COMB).

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

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

6.6.2.19 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.

6.6.3 Security

Menu Item	Options	Description
TrEE Protocol Version	1.0 / 1.1	TrEE Protocol Version: 1.0 or 1.1.
TPM Availability	Available / Hidden	When Hidden, do not exposes TPM to 0.
Clear TPM	[ ] / [X]	Clear TPM. Removes all TPM context associated with a specific Owner.
Set Supervisor Password	123456	Install or change the BIOS password. The length of password must be greater than one and smaller or equal ten characters.

6.6.4 Power

Menu Item	Options	Description
ACPI S3	Enabled / Disabled	Enable/Disable ACPI S1/S3 Sleept state.
Wake on PME	Enabled / Disabled	Determines the action taken when the system power is off and a PCI Power Management Enable (PME) wake up event occurs.
Wake on Modem Ring	Enabled / Disabled	Determines the action taken when the system power is off and a modem connected to the serial port is ringing.
Auto Wake on S5	Disabled / By Every Day / By Day of Month	Auto wake on S5, By Day of Month or Fixed time of every day.
S5 Long Run Test	Enabled / Disabled	Enable: force to enable RTC S5 wake up, even if OS disables it. Support ipwrtest to do RTC S5 wakeup.

6.6.5 Boot

Menu Item	Options	Description
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.

Menu Item	Options	Description
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 Note: This option is only configurable if 'Network Stack' is enabled.
Power up In Standby Support	Enabled / Disabled	Enable or disable the Power Up in Standby Support (PUIS). The PUIS feature allows devices to be powered-up into the Standby power management state to minimize inrush current at power-up and to allow the host to sequence the spin-up of devices.
Storage PCI Option Rom access right Support	Enabled / Disabled	Disable or enable storage PCI option rom access right. This feature will enable or disable storage PCI option rom being load and dispatched.
ESATA drive boot access right Support	Enabled / Disabled	Disable or enable ESATA drive boot access right. This feature will allow or deny boot up an ESATA storage device.
Add Boot Options	First / Last / Auto	Position in Boot Order for Shell, Network and Removables.
ACPI Selection	Acpi1.0B / Acpi3.0 / Acpi4.0 / Acpi5.0 / Acpi6.0 / Acpi6.1	Select booting to ACPI selection.
USB Boot	Enabled / Disabled	Enable or disable booting to USB boot device.
UEFI OS Fast Boot	Enabled / Disabled	If enabled the system firmware does not initialize keyboard and check for firmware menu key.
USB Hot Key Support	Enabled / Disabled	Enable or disable to support USB hot key while booting. This will decrease the time needed to boot the system, 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	See submenu	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.

7. BIOS – UPDATE

The uEFI BIOS update instruction serves to guarantee a proper way to update the uEFI BIOS on the TQMx110EB.
Please read the entire instructions before beginning the BIOS update.
By disregarding the information you can destroy the uEFI BIOS on the TQMx110EB!
This document will guide the customer to update the uEFI BIOS on the TQMx110EB by using the Insyde Flash Firmware Tools.
The InsydeH2O Tools are only available on request.
Please contact support@tq-group.com for more information about the BIOS Tools and the latest uEFI BIOS version for the TQMx110EB.

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

7.1.1 Step 1: Preparing USB Stick

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

- H2OFFT-Sx64.efi (Flash Firmware Tool from Insyde for update via UEFI Shell)
  - Be sure to have H2OFFT Version 200.02.00.02 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

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

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

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

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

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

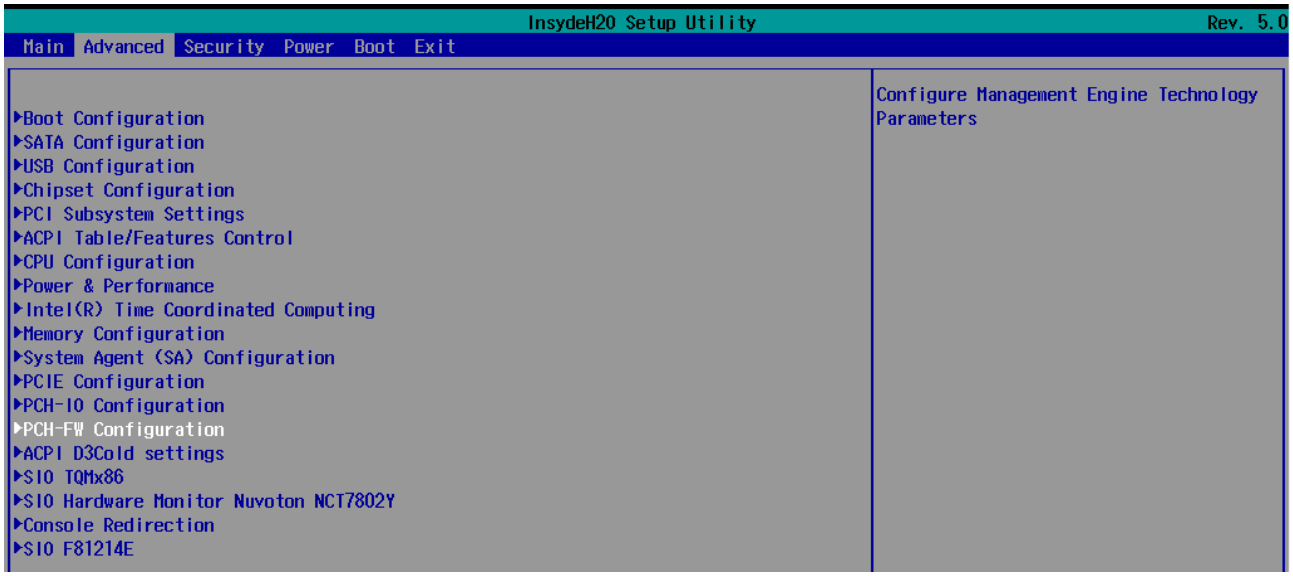


Figure 10: PCH-FW Configuration menu

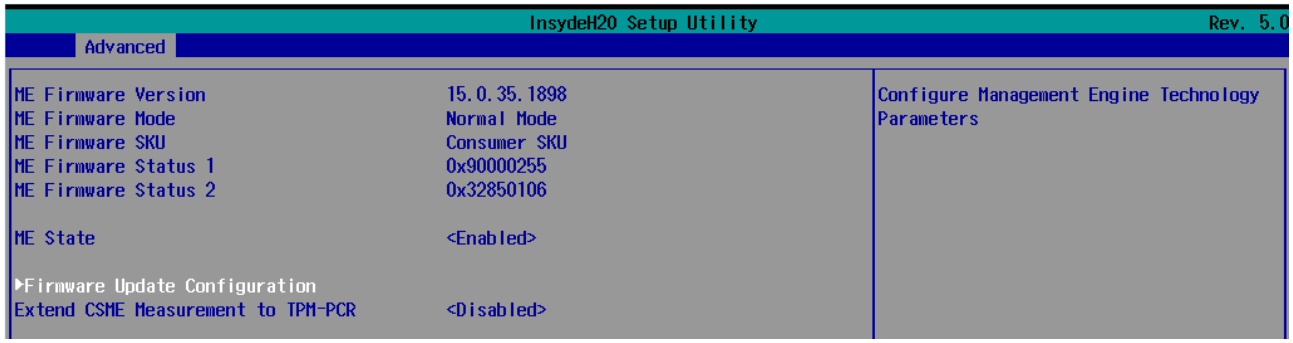


Figure 11: Firmware Update Configuration menu

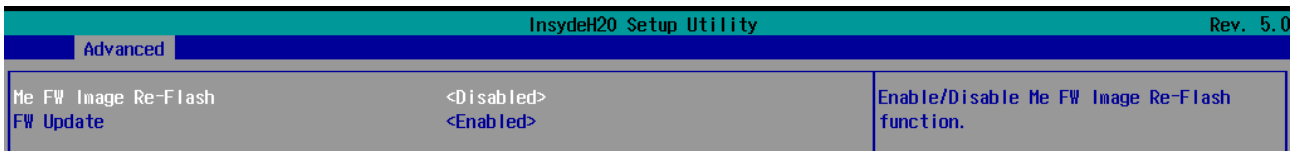


Figure 12: ME FW Image Re-Flash option

7.1.3 Step 3a: Updating uEFI BIOS via EFI Shell

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

Figure 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 tqmx110eb`") to execute the Insyde BIOS update tool:

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

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

Figure 14: EFI Shell uEFI BIOS Update

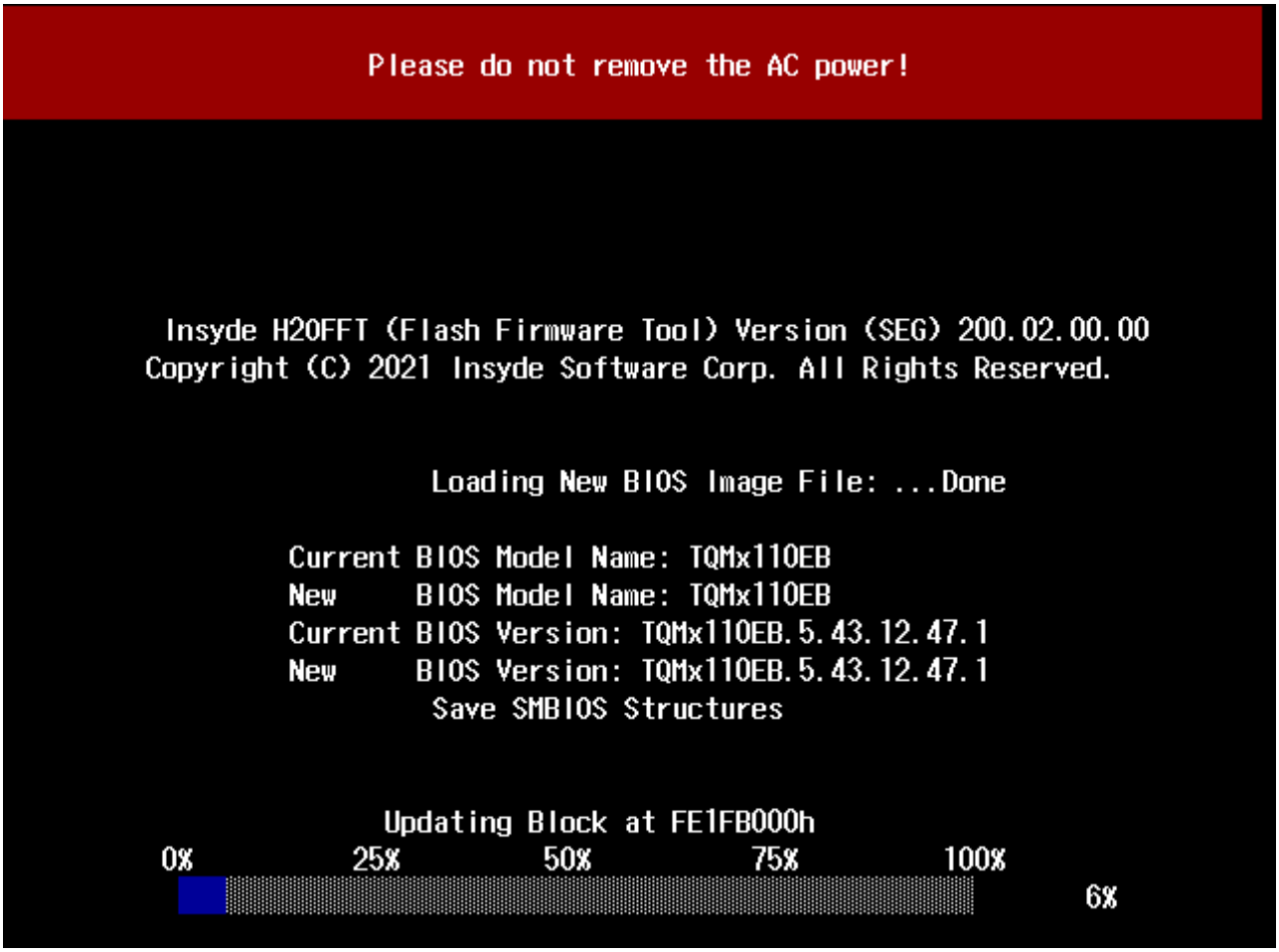


Figure 15: Screen during BIOS Update

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

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

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

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

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

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

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

7.1.5 Step 4: BIOS update check on the TQMx110EB Module

After the uEFI BIOS update, the new uEFI BIOS configures the complete TQMx110EB hardware and this results in some reboots and the first boot time takes longer (up to 1 minute).
The TQMx110EB 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.

Figure 16: TQMx110EB Debug LED

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

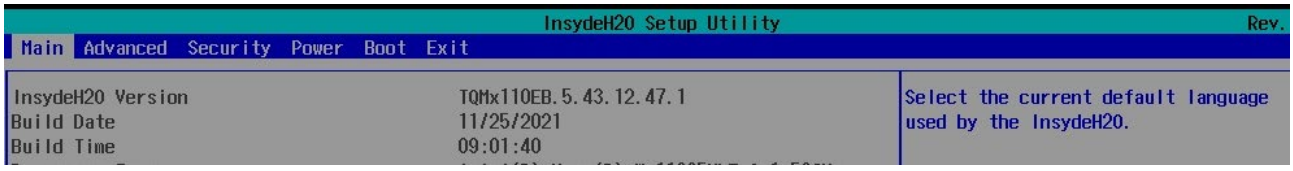


Figure 17: EFI BIOS Main Menu

8. SAFETY REQUIREMENTS AND PROTECTIVE REGULATIONS

8.1 EMC

The TQMx110EB was developed according to electromagnetic compatibility requirements (EMC). Depending on the target system, anti-interference measures may still be necessary to guarantee the adherence to the limits for the overall system.

8.2 ESD

In order to avoid interspersion on the signal path from the input to the protection circuit in the system, the protection against electrostatic discharge should be arranged directly at the inputs of a system. As these measures always have to be implemented on the carrier board, no special preventive measures were done on the TQMx110EB.

8.3 Shock & Vibration

The TQMx110EB is designed to be insensitive to shock and vibration and impact.

8.4 Operational Safety and Personal Security

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

8.5 Reliability and Service Life

The MTBF according to MIL-HDBK-217F N2 is approximately 362546 h, Ground Benign, @ +40 °C.

8.5.1 RoHS

The TQMx110EB is manufactured RoHS compliant.

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

8.5.2 WEEE®

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

8.6 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.

8.7 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 TQMx110EB must therefore always be seen in conjunction with the complete device. The available standby and sleep modes of the components on the TQMx110EB enable compliance with EuP requirements for the TQMx110EB.

8.8 Battery

No batteries are assembled on the TQMx110EB.

8.9 Packaging

By environmentally friendly processes, production equipment and products, we contribute to the protection of our environment. To be able to reuse the TQMx110EB, 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 TQMx110EB is delivered in reusable packaging.

8.10 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 21: Acronyms

Acronym	Meaning
AHCI	Advanced Host Controller Interface
AMI	American Megatrends, Inc.
ATA	Advanced Technology Attachment
AVC	Advanced Video Coding
BIOS	Basic Input/Output System
CAN	Controller Area Network
CMOS	Complementary Metal Oxide Semiconductor
CODEC	Code/Decode
COM	Computer-On-Module
CPU	Central Processing Unit
CSM	Compatibility Support Module
cTDP	Configurable Thermal Design Power
DC	Direct Current
DDC	Display Data Channel
DDI	Digital Display Interface
DDR	Double Data Rate
DMA	Direct Memory Access
DP	DisplayPort
DVI	Digital Visual Interface
DXVA	DirectX Video Acceleration
EAPI	Embedded Application Programming Interface
ECC	Error-Correcting Code
EDID	Extended Display Identification Data
eDP	embedded DisplayPort
eDRAM	Embedded DRAM
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFI	Extensible Firmware Interface
EMC	Electromagnetic Compatibility
ESD	Electrostatic Discharge
FAE	Field Application Engineer
FIFO	First In First Out
flexiCFG	Flexible Configuration
FPGA	Field Programmable Gate-Array
FR-4	Flame Retardant 4
GPIO	General Purpose Input/Output
HD	High Definition
HDA	High Definition Audio
HDMI	High Definition Multimedia Interface
HEVC	High Efficiency Video Coding
HSP	Heat Spreader
HT	Hyper-Threading
I	Input
I PD	Input with internal Pull-Down resistor
I PU	Input with internal Pull-Up resistor
I/O	Input/Output
I^2C	Inter-Integrated Circuit
IDE	Integrated Drive Electronics
IEC	International Electrotechnical Commission
IoT	Internet of Things
IP00	Ingress Protection 00
IRQ	Interrupt Request
JEIDA	Japanese Electronics Industry Development Association
JPEG	Joint Photographic Experts Group
JTAG®	Joint Test Action Group
LED	Light Emitting Diode
LPC	Low Pin Count
LVDS	Low Voltage Differential Signal

9.1 Acronyms and Definitions (continued)

Table 21: Acronyms (continued)

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

9.2 References

Table 22: Further Applicable Documents and Links

No.	Name	Rev., Date	Company
(1)	11th Generation Intel® Core™ and XEON® H series Product Brief	–	Intel
(2)	PICMG® COM Express™ Module Base Specification	Rev. 3.0, March 31, 2017	PICMG
(3)	PICMG® COM Express™ Carrier Design Guide	Rev. 2.0, Dec. 6, 2013	PICMG
(4)	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