TQMx80UC
User's Manual

TQMx80UC UM 0102
2020-02-04

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

TABLE OF CONTENTS (continued)

TABLE DIRECTORY

ILLUSTRATION DIRECTORY

REVISION HISTORY

Rev.	Date	Name	Pos.	Modification
0100	2019-07-30	KG		First release
0101	2020-01-20	FP	All Table 2 Table 12	Typo, expression Added Signals C67 and C97 corrected (swapped)
0102	2020-02-04	FP	Table 2	TQMx80UC-AC: eMMC size corrected

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 TQMx80UC 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 (4), 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 (3), (5).

2. INTRODUCTION

Based on the internationally established PICMG® standard COM Express™ (COM.0 R3.0), the TQMx80UC 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 8th Generation Intel® Core™ 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 TQMx80UC board design is prepared to also support the next Intel 9th Generation Intel® Core™ U Embedded series with up to 6 processor cores (Comet Lake-U).

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 TQMx80UC:

Processor:
8th Generation Intel® Core™ UE series („Whiskey Lake-U")

- Intel® Core™ i7-8665UE 4 × 1.7 GHz / 4.4 GHz Turbo, 8 MB Cache, 15 W (cTDP 12.5 W and 25 W)
- Intel® Core™ i5-8365UE 4 × 1.6 GHz / 4.1 GHz Turbo, 6 MB Cache, 15 W (cTDP 12.5 W and 25 W)
- Intel® Core™ i3-8145UE 2 × 2.2 GHz / 3.9 GHz Turbo, 4 MB Cache, 15 W (cTDP 12.5 W and 25 W)
- Intel® Celeron™ 4305UE 2 × 2.0 GHz, 2 MB Cache, 15 W (cTDP 12.5 W)

Memory:

- 2 × DDR4 SO-DIMM socket with max. 64 Gbyte, dual channel DDR4 2400 MT/s SO-DIMM modules
- eMMC 5.1 on-board flash up to 128 Gbyte
- Support of Intel® Optane™ memory technology via PCIe
- EEPROM: 32 kbit (24LC32)

Graphics:

- 2 × Digital Display Interface / DP++ with up to 4K; DisplayPort 1.2a with support for Multi-Stream Transport (MST)
- 1 × Embedded Digital Display Interface (eDP) or dual LVDS interface (eDP 1.4 or dual LVDS)

Peripheral interfaces:

- 1 × Gigabit Ethernet (Intel® i219)
- 4 × USB 3.1 Gen 2 (up to 10 Gb/s) with USB 3.0 and 2.0 backward compatibility
- 8 × USB 2.0
- 2 × SATA Gen3 (up to 6 Gb/s)
- 8 × PCIe 3.0 (up to 8 Gb/s) (8 (×1), 4 (×2), or 2 (×4))
- 1 × PCIe 3.0 PEG port (up to 8 Gb/s) (1 (x1))
- 1 × LPC bus
- 1 × Intel® HD audio (HDA)
- 1 × I²C, (2nd I²C optional) (master/slave capable)
- 1 × SMBus
- 1 × SPI (for external uEFI BIOS flash)
- 2 × Serial port (Rx/Tx, legacy compatible), 4-wire (Rx/Tx/RTS/CTS) optionally through TQ-flexiCFG
- 8 × GPIO through TQ-flexiCFG or 1 × SD card interface (multiplexed, default GPIO)

Security components:

- TPM discrete SLB9665 TPM 2.0 controller or internal firmware TPM (FTPM)

Others:

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

Power supply voltage:

- 8.5 V to 20 V
- 5 V Standby (optional)
- 3 V Battery for RTC

Environment:

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

Form factor / dimensions:

- COM Express™ Compact, Type 6, 95 × 95 mm²

2.2 Compliance

The TQMx80UC complies with PICMG® COM Express™ Module Base Specification (COM.0 R3.0). (Compact, Type 6, 95 × 95 mm²).

2.3 Versions

The TQMx80UC is available in several standard configurations

Table 2: TQMx80UC Standard Configurations and Features

Feature	TQMx80UC-AA	TQMx80UC-AB	TQMx80UC-AC	TQMx80UC-AD	TQMx80UC-AE	TQMx80UC-AF	TQMx80UC-AG	TQMx80UC-AH	TQMx80UC-AI
CPU	Quad	Quad	Dual	Dual	Dual	Quad	Quad	Quad	Dual
Intel	Core™ i7-8665UE	Core™ i5-8365UE	Core™ i3-8145UE	Core™ i3-8145UE	Celeron™ 4305UE	Core™ i7-8665UE	Core™ i7-8665UE	Core™ i5-8365UE	Celeron™ 4305UE
CPU TDP	15 Watt	15 Watt	15 Watt	15 Watt	15 Watt	15 Watt	15 Watt	15 Watt	15 Watt
CPU Clock (Burst)	4.4 GHz	4.1 GHz	3.9 GHz	3.9 GHz	2.0 GHz	4.4 GHz	4.4 GHz	4.1 GHz	2.0 GHz
CPU Clock (Base)	1.7 GHz	1.6 GHz	2.2 GHz	2.2 GHz	2.0 GHz	1.7 GHz	1.7 GHz	1.6 GHz	2.0 GHz
Graphics	Intel® UHD Graphics 620	Intel® UHD Graphics 620	Intel® UHD Graphics 620	Intel® UHD Graphics 620	Intel® UHD Graphics 620	Intel® UHD Graphics 620	Intel® UHD Graphics 620	Intel® UHD Graphics 620	Intel® UHD Graphics 620
L2 Cache	8 MB	6 MB	4 MB	4 MB	4 MB	8 MB	8 MB	6 MB	4 MB
Heat spreader	TQMx80UC-HSP-AA	TQMx80UC-HSP-AA	TQMx80UC-HSP-AA	TQMx80UC-HSP-AA	TQMx80UC-HSP-AA	TQMx80UC-HSP-AA	TQMx80UC-HSP-AA	TQMx80UC-HSP-AA	TQMx80UC-HSP-AA
Heatsink incl. fan	TQMx80UC-KK-AA	TQMx80UC-KK-AA	TQMx80UC-KK-AA	TQMx80UC-KK-AA	TQMx80UC-KK-AA	TQMx80UC-KK-AA	TQMx80UC-KK-AA	TQMx80UC-KK-AA	TQMx80UC-KK-AA
DRAM / SODIMM	8 / 16 / 32 / 64 GB	8 / 16 / 32 / 64 GB	8 / 16 / 32 / 64 GB	8 / 16 / 32 / 64 GB	8 / 16 / 32 / 64 GB	8 / 16 / 32 / 64 GB	8 / 16 / 32 / 64 GB	8 / 16 / 32 / 64 GB	8 / 16 / 32 / 64 GB
On-board eMMC	32 GB	32 GB	0 GB	8 GB	8 GB	32 GB	64 GB	32 GB	8 GB
Operating Temperature	0 °C to +60 °C	0 °C to +60 °C	0 °C to +60 °C	0 °C to +60 °C	0 °C to +60 °C	0 °C to +60 °C	0 °C to +60 °C	0 °C to +60 °C	0 °C to +60 °C
Screening Option	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TPM 2.0	0	0	0	1	0	0	0	0	0
Independent displays	3	3	3	3	3	3	3	3	3
LVDS (1920×1080@60 Hz)	0	0	0	1	0	1	0	1	1
eDP (4096×2304@60 Hz)	1	1	1	0	1	0	1	0	0
DP (1920×1080@60 Hz)	1	1	1	1	1	1	1	1	1
HDMI (1920×1080@24 Hz)	1	1	1	1	1	1	1	1	1
GbE	1	1	1	1	1	1	1	1	1
USB2.0 host	8	8	8	8	8	8	8	8	8
USB3.1 host	4	4	4	4	4	4	4	4	4
SATA-III	2	2	2	2	2	2	2	2	2
PCIe Gen3 ×1	8	8	8	8	8	8	8	8	8
PEG ×1	1	1	1	1	1	1	1	1	1
I2C / SPI	1 / 1	1 / 1	1 / 1	1 / 1	1 / 1	1 / 1	1 / 1	1 / 1	1 / 1
HAD	1	1	1	1	1	1	1	1	1
UART / GPIO / SDIO	2 / 8 / 1	2 / 8 / 1	2 / 8 / 1	2 / 8 / 1	2 / 8 / 1	2 / 8 / 1	2 / 8 / 1	2 / 8 / 1	2 / 8 / 1

2.3 Versions (continued)

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
- Custom specific GPIO configuration through TQ-flexiCFG
- LVDS / eDP configuration
- Customized BIOS
- I-Temp (–40 °C to +85 °C), with screening

2.4 Accessories

- **TQMx80UC-HSP**
  Heat spreader for TQMx80UC, according to COM Express™ specification.
- **Evaluation platform MB-COME6-3**
  Mainboard for COM Express™ Basic and Compact, Type 6, 170 × 170 mm², with the following interfaces:
  - 3 × DP
  - LVDS
  - 2 × Gbit Ethernet
  - 4 × USB 3.1
  - 1 × COM
  - Audio
  - M.2 for I/O
  - M.2 for SSD
  - 2.5“ SSD
  - SD card
  - Riser extension with PCIe
  - Fan
  - Debug
- **Debug module**
  POST debug card for TQMx80UC, see3.6.3.

3. FUNCTION

3.1 Block Diagram

The following illustration shows the TQMx80UC block diagram.

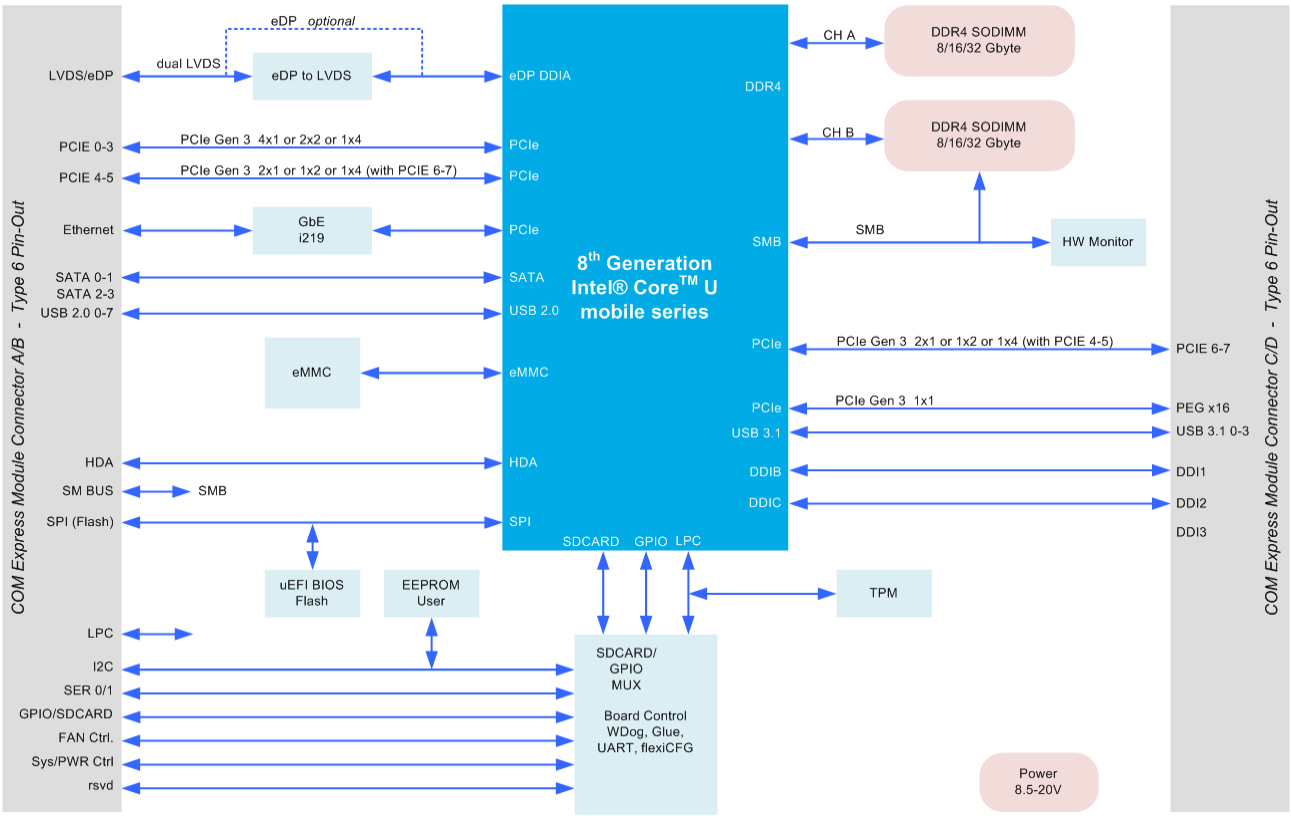


Illustration 1: TQMx80UC Block Diagram

3.2 Electrical Characteristics

3.2.1 Supply Voltage

The TQMx80UC supports a wide-range voltage input from 8.5 V to 20 V.

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

Wide input:	8.5 V to 20 V	maximum input ripple:	±100 mV	(0 °C to +60 °C)
Standard input:	8.5 V to 12.6 V	maximum input ripple:	±100 mV	(–40 °C to +85 °C)
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 msec to 20 msec (0.1 msec ≤ Rise Time ≤ 20 msec).
The increase of each DC output voltage has to be smooth and continuous from 10 % to 90 % of its final set point within the regulation range.

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 TQMx80UC voltage and power specifications.

The values were measured with two power supplies; one for the TQMx80UC and the other one for the MB-COME6-3 COM Express™ carrier board.

The power consumption of each TQMx80UC was measured running Windows® 10, 64-bit and a dual DDR4 SO-DIMM configuration (2 × 8 Gbyte). All measurements were done at a temperature of +25 °C and an input voltage of +12 V.

The power consumption of the TQMx80UC 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 TQMx80UC 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 (cTDP up mode enabled):**
  These values show the maximum cTDP up 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 28sec)**
  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 sec) when the processor is in the turbo mode. This value should be used for designing the power supply for the TQMx80UC. Ethernet port is connected (1000Base-T Speed).

The following table shows the TQMx80UC power consumption with different CPUs.

Table 3: TQMx80UC Power Consumption

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 cTDP up max. load	Win10, 64-bit Max load (Turbo mode)
i7-8665UE	4.0 mW	200 mW	2.5 W	16 W	19 W	30 W	55 W
i5-8365UE	4.0 mW	200 mW	2.5 W	16 W	19 W	30 W	55 W
i3-8145UE	4.0 mW	200 mW	2.5 W	16 W	19 W	30 W	32 W
4305UE	4.0 mW	200 mW	2.5 W	14 W	16 W	–	–

Note: Power requirement	
	The power supplies on the carrier board for the TQMx80UC have to be designed with enough reserve. The carrier board should be able to provide at least twice the maximum TQMx80UC workload power. The TQMx80UC supports several low-power states. The carrier board power supply has to be stable, even with no load.

3.2.3 Real Time Clock Power Consumption

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

Table 4: RTC Current Consumption

Mode	Voltage	Current
8th Generation Intel® Core™ UE series integrated RTC	3.0 V	2 µA

The current consumption of the RTC in the 8th Generation Intel® Core™ UE series Product Family Datasheet is specified with 6 µA in average, but the values measured on several TQMx80UC were lower.

3.3 Environmental Conditions

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

Attention: Maximum operating temperature	
	Do not operate the TQMx80UC 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 TQMx80UC supports the 8th Generation Intel® Core™ UE Embedded processor series (Whiskey Lake-U).
The TQMx80UC board design is prepared to also support the 9th Generation Intel® Core™ UE Embedded series with up to 6 processor cores (Comet Lake-U).

The following list illustrates some key features of the 8th Generation Intel® Core™ UE Embedded processor series:

- Quad and dual processor cores
- Intel® Hyper-Threading Technology (Intel® HT Technology)
- Intel® Streaming SIMD Extensions 4.2 (Intel® SSE4.2)
- Intel® Advanced Vector Extensions 2.0 (Intel® AVX2)
- Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
- Intel® 64 Architecture
- Intel® Turbo Boost Technology 2.0
- Intel® Configurable Thermal Design Power (Intel® cTDP up and down)
- Intel® Enhanced Intel® SpeedStep® technology
- Up to 8 Mbyte Cache
- Intel® UHD Graphics 610 / 620
- High Definition Content Protection (HDCP) 2.2
- Three independent displays

Table 5: 8th Generation Intel® Core™ UE i7, i5, i3 and Celeron™ Embedded series

Mode	Core™ i7-8665UE	Core™ i5-8365UE	Core™ i3-8145UE	Celeron™ 4305UE
Processor Cores / Threads	4 / 8	4 / 8	2 / 4	2 / 2
Cache	8 Mbyte	6 Mbyte	4 Mbyte	2 Mbyte
Core Base frequency	1.7 GHz	1.6 GHz	2.2 GHz	2.0 GHz
Core Base frequency (cTDP up)	2.0 GHz	1.8 GHz	2.4 GHz	–
Core Base frequency (cTDP down)	1.3 GHz	1.1 GHz	1.6 GHz	0.8 GHz
Core Max. Turbo frequency	4.4 GHz	4.1 GHz	3.9 GHz	2.0 GHz
$T_{junction}$	0 °C to +100 °C	0 °C to +100 °C	0 °C to +100 °C	0 °C to +100 °C
Memory speed DDR4	2400 MT/s	2400 MT/s	2400 MT/s	2133 MT/s
Max. memory	64 Gbyte	64 Gbyte	64 Gbyte	64 Gbyte
Memory configuration	Dual, no ECC	Dual, no ECC	Dual, no ECC	Dual, no ECC
Graphics	UHD Graphics 620 (GT2)	UHD Graphics 620 (GT2)	UHD Graphics 620 (GT2)	UHD Graphics 610 (GT1)
Graphics Execution Units	24	24	24	12
Graphics Base frequency	0.3 GHz	0.3 GHz	0.3 GHz	0.3 GHz
Graphics Turbo frequency	1.15 GHz	1.05 GHz	1.0 GHz	1.0 GHz
Thermal Design Power (TDP nominal)	15 W	15 W	15 W	15 W
Configurable Thermal Design Power (cTDP up)	25 W	25 W	25 W	–
Configurable Thermal Design Power (cTDP down)	12.5 W	12.5 W	12.5 W	12.5 W
Processor Power Limit 2 (PL2)	51.0 W	51.0 W	29.0 W	29.0 W
Intel® vPro Technology	vPro	vPro	–	–
Intel® Hyper-Threading Technology	Yes	Yes	Yes	No
Intel® Turbo Boost Technology	Yes	Yes	Yes	No
Chipset	300 series	300 series	300 series	300 series

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, and i3 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 (15 W).
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.
3. The cTDP up mode specifies a higher processor power consumption and a higher guaranteed frequency versus the nominal mode. This mode can be selected for high performance applications with optimized cooling solutions up to 25 W.

The cTDP up feature is only available on the Intel® Core™ i7, i5, and i3 processor versions.

The cTDP function can be configured in the uEFI BIOS, the default setting is "nominal".

3.4.2 Graphics

The 8th Generation Intel® Core™ UE Embedded processor series includes an integrated Intel® HD graphics accelerator.

It provides excellent 2D / 3D graphics performance with triple simultaneous display support.

The following list illustrates some key features of the 8th Generation Intel® Core™ UE Embedded processor:

- Graphics Technology GT2 with 24 Execution Units UHD Graphics 620
- Graphics Technology GT1 with 12 Execution Units UHD Graphics 610
- Hardware accelerated video decoding/encoding for AVC/VC-1/MPEG2/HEVC/VP8/JPEG
- Direct3D* 12, DirectX* 12 support
- OpenGL* 4.5, OpenCL* 2.0 support

The TQMx80UC supports two external Digital Display Interfaces (DDI1 and DDI2) and one internal display, either dual channel LVDS or eDP interface at the COM Express™ connector, depending on TQMx80UC and carrier configuration.

The 8th Generation Intel® Core™ UE Embedded processor series supports up to three displays at the same time.

Table 6: Maximum Resolution in Triple Display Configuration

Display	Maximum Display Resolution
LVDS	1920 × 1200 @ 60 Hz
eDP	4096 × 2304 @ 60 Hz
DP	4096 × 2304 @ 60 Hz
HDMI 1.4	4096 × 2160 @ 24 Hz
HDMI 2.0 (LSPCON)	4096 × 2160 @ 60 Hz

*HDMI 2.0 support is possible via a Level Shifter and Protocol Converter (LSPCON) on the carrier.

3.4.3 Chipset

The 8th Generation Intel® Core™ UE Embedded processor series includes an integrated chipset with the Intel® Platform Controller Hub (PCH) 300 series.

3.4.4 Memory

3.4.4.1 DDR4 SDRAM

The TQMx80UC supports a dual-channel DDR4 memory, running at up to 2400 MT/s.
It provides two 260-pin DDR4 SO-DIMM sockets for two DDR4 SO-DIMM modules that support system memory configurations of 8 Gbyte, 16 Gbyte, 32 Gbyte or 64 Gbyte.
DDR4 supports an operating voltage of 1.2 V, resulting in reduced power consumption and heat dissipation compared to DDR3.

Note: DDR4 SO-DIMM modules	
	Only DDR4 SO-DIMM modules qualified by TQ-Systems are authorized for use with the TQMx80UC. DDR4 SO-DIMM modules not released by TQ-Systems may cause functional issues.

On customer request a soldered memory configurations can be made available.

3.4.4.2 eMMC

The TQMx80UC supports up to 128 Gbyte on-board eMMC flash devices, compatible with JESD84-B50 (eMMC 5.1).
The eMMC flash device can be enabled in the uEFI BIOS, the default configuration in the uEFI BIOS is disabled.
uEFI BIOS configuration: *Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ SCS Configuration*

Note: eMMC Operation System installation	
	The on-board eMMC flash requires pre-configuration via EFI Shell before Operating System installation (using e.g. diskpart utility).

3.4.4.3 SPI Boot Flash

The TQMx80UC 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 TQMx80UC supports a COM Express™ Module EEPROM. The 2 kbit EEPROM AT24C32C 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 TQMx80UC includes a standard RTC (Motorola MC146818B) integrated in the Intel PCH.

3.4.6 Trusted Platform Module

The TQMx80UC supports the Trusted Platform Module (TPM) 2.0 (Infineon SLB9665 controller).
The 8th Generation Intel® Core™ UE Embedded processor 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 TQMx80UC 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 TQMx80UC 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 TQMx80UC 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
- M.2 device select (PCIe or SATA mode) via GPIO
- 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

The TQMx80UC supports the ultra-deep power state Green ECO-Off. In this configuration all DC/DC power supplies on the TQMx80UC 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 TQMx80UC 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 7: 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 with auto detection for M.2 PCI Express / SATA interface

Note: PCI Express port configuration	
	A maximum of five PCI Express root ports can be enabled.

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) or SATA interface.

To support Intel® Optane™ or Rapid Storage Technology, the four PCI Express lanes of the 8th Generation Intel® Core™ UE Embedded processor series are connected to COM Express™ connector port 4 to 7 and used on an M.2 PCI Express socket.

The COM Express™ Specification does not provide signal definitions for the M.2 PCI Express / SATA select signal.
The TQMx80UC supports the missing PCI Express / SATA select signal to the COM Express™ connector, to solve this limitation.

Table 8: PCI Express port 4 – 7 M.2 PCI Express / SATA configuration options

COM Express Signal	COM Express Pin	TQMx80UC	Remark
RSVD	D97	M2_PE/SATA_DET PCI Express = 1 (default) SATA = 0	3.3 V input

3.5.2 PCI Express for Graphics (PEG)

At the COM Express™ connector the TQMx80UC supports one x1 Gen 3 PCI Express Graphics port with 8 Gb/s speed.
The PCI Express PEG lanes 1 – 15 are not used.

3.5.3 Gigabit Ethernet

The TQMx80UC provides an Intel® i219 Ethernet controller with 10/100/1000 Mbps speed.
Features of the Intel® i219 Ethernet controller:

- Automatic speed configuration 10 BASE-T / 100 BASE-TX / 1000 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)

3.5.4 Serial ATA

The TQMx80UC supports two 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 two 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.

3.5.5 Digital Display Interface

The TQMx80UC supports three Digital Display Interfaces at the COM Express™ connector DDI1, DDI2 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) or eDP as an assembly option.
Maximum display resolutions:

- DisplayPort 1.2a resolution up to 4096 × 2304 @ 60 Hz
- HDMI 1.4 up to 4096 × 2160 @ 24 Hz
- HDMI 2.0 up to 4096 × 2160 @ 60 Hz*
- DVI up to 4096 × 2160 @ 24 Hz (HDMI without Audio)
- eDP up to 4 lanes eDP 1.4 up to 4096 × 2304 @ 60 Hz
- LVDS up to 1920 × 1200 @ 60 Hz in dual channel LVDS mode

*HDMI 2.0 support is possible via a Level Shifter and Protocol Converter (LSPCON) on the carrier.

3.5.6 LVDS Interface

The TQMx80UC supports an LVDS 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 LVDS data packing can be configured either in VESA or JEIDA format.
To support panels without EDID ROM, the eDP-to-LVDS bridge can emulate EDID ROM behaviour avoiding specific changes in system video BIOS.
Please contact support@tq-group.com for further information about the LVDS configuration.

3.5.7 USB Interfaces

The TQMx80UC supports eight USB 2.0 and four USB 3.1 Gen 2 ports with data rate up to 10 Gbps at the COM Express™ connector. All USB 3.1 Gen 2 ports are configurable to USB 3.1 Gen 1 (5 Gbps).
Care must be taken in the COM Express™ carrier design, the carrier must support the USB 3.1 Gen 2 (10 Gbps) high speed standard.

Attention: USB 3.1 Gen 2 (10 Gbps) carrier design	
	The COM Express™ specification Revision 3.0 only supports the USB 3.1 Gen 1 (5 Gbps) data rate. If the COM Express™ carrier is not designed for the USB 3.1 Gen 2 (10 Gbps) operation, the USB 3.1 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 3.1 SuperSpeedPlus port 0. The USB 2.0 port 1 must be paired with USB 3.1 SuperSpeedPlus port 1. The USB 2.0 port 2 must be paired with USB 3.1 SuperSpeedPlus port 2. The USB 2.0 port 3 must be paired with USB 3.1 SuperSpeedPlus port 3.

To support more than four USB 3.1 ports the PCI Express I/O ports can be configured to USB 3.1.
With a customized BIOS the PCI Express lane can be configured to USB 3.1.

3.5.8 SD Card Interface

The TQMx80UC provides an SD card interface for 4-bit SD/MMC cards at the COM Express™ connector.
The SD card signals are shared with the GPIO signals and can be configured via the BIOS.
The default configuration at the COM Express™ connector is with GPIO signals.
The SD card interface can be enabled in the uEFI BIOS, the default configuration in the uEFI BIOS is disabled.
uEFI BIOS configuration: *Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ SCS Configuration*

3.5.9 General Purpose Input / Output

The TQMx80UC 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 default configuration at the COM Express™ connector is with GPIO signals.
The signals can also be used for special functions (see 3.4.8).

3.5.10 High Definition Audio Interface

The TQMx80UC 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™ is not connected. The Audio Codec is assembled on the carrier board.

3.5.11 LPC Bus

The TQMx80UC supports a Low Pin Count (LPC) legacy bus for I/O expansion.
The LPC bus Direct Memory Access (DMA) is not supported.

3.5.12 I²C Bus

The TQMx80UC 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.

3.5.13 SMBus

The TQMx80UC provides a System Management Bus (SMBus).

3.5.14 Serial Peripheral Interface

The TQMx80UC provides a Serial Peripheral Interface (SPI) interface.
The SPI interface can only be used for SPI boot Flash devices.

3.5.15 Serial Ports

The TQMx80UC 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 9: Serial Port COM Express™ Port Mapping

COM Express™ Signal	COM Express™ Pin	TQMx80UC	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 TQMx80UC the protection circuit is removed by default and the serial ports provide transfer rates of up to 115 kbaud. Therefore the TQMx80UC can only be used in a COM Express™ COM.0 2.0 and 3.0 Type 6 pin-out carrier board.

3.5.16 Watchdog Timer

The TQMx80UC 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 TQMx80UC 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.

3.6.2 Debug Header

The TQMx80UC 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.

Illustration 2: TQM Debug Card

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

3.6.4 Debug Module LED

The TQMx80UC includes a dual colour LED providing boot and BIOS information.
The following table illustrates some LED boot messages:

Table 10: 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

3.7 COM Express™ Connector Pinout

This section describes the TQMx80UC 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 11: 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 TQMx80UC.

3.7.2 COM Express™ Connector Pin Assignment

Table 12: COM Express™ Connector Pin Assignment

Pin	Pin-Signal	Description	Type	Remark
A1	GND (FIXED)	Ground	GND	
A2	GBE0_MDI3–	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A3	GBE0_MDI3+	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A4	GBE0_LINK100#	Gigabit Ethernet Controller 0 100 Mbit / sec link indicator	OD	
A5	GBE0_LINK1000#	Gigabit Ethernet Controller 0 1000 Mbit / sec link indicator	OD	
A6	GBE0_MDI2–	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A7	GBE0_MDI2+	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A8	GBE0_LINK#	Gigabit Ethernet Controller 0 link indicator	OD	
A9	GBE0_MDI1–	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A10	GBE0_MDI1+	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A11	GND (FIXED)	Ground	GND	
A12	GBE0_MDI0–	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A13	GBE0_MDI0+	Gigabit Ethernet Controller 0: Media Dependent Interface	IO	
A14	GBE0_CTREF	Reference voltage for Carrier Board Ethernet channel 0	Power	
A15	SUS_S3#	Indicates system is in Suspend to RAM state. Active low output.	O PD	TQ-flexiCFG
A16	SATA0_TX+	SATA differential transmit pair	O	
A17	SATA0_TX–	SATA differential transmit pair	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 pair	I	
A20	SATA0_RX–	SATA differential receive pair	I	
A21	GND (FIXED)	Ground	GND	
A22	SATA2_TX+	SATA differential transmit pair	O	N/A
A23	SATA2_TX–	SATA differential transmit pair	O	N/A
A24	SUS_S5#	Indicates system is in Soft Off state. Active low output.	O PD	TQ-flexiCFG
A25	SATA2_RX+	SATA differential receive pair	I	N/A
A26	SATA2_RX–	SATA differential receive pair	I	N/A
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 pair	IO	
A37	USB6+	USB differential pair	IO	
A38	USB_6_7_OC#	USB over-current sense, USB channels 6 and 7	I PU	
A39	USB4–	USB differential pair	IO	
A40	USB4+	USB differential pair	IO	
A41	GND (FIXED)	Ground	GND	
A42	USB2–	USB differential pair	IO	
A43	USB2+	USB differential pair	IO	
A44	USB_2_3_OC#	USB over-current sense, USB channels 2 and 3	I PU	
A45	USB0–	USB differential pair	IO	
A46	USB0+	USB differential pair	IO	
A47	VCC_RTC	Real-time clock circuit-power input. Nominally +3.0 V	Power	
A48	RSVD	Reserved	NC	TQ-flexiCFG
A49	GBE0_SDP	Gigabit Ethernet Controller 0 Software-Definable Pin	I/O	N/A
A50	LPC_SERIRQ/ESPI_CS1#	LPC serial interrupt	IOPU	LPC
A51	GND (FIXED)	Ground	GND	
A52	PCIE_TX5+	PCI Express differential transmit pair	O	
A53	PCIE_TX5–	PCI Express differential transmit pair	O	
A54	GPI0/SD_DATA0	GPI0 / SDIO Data lines	I PU	GP or SD card
A55	PCIE_TX4+	PCI Express differential transmit pair	O	

3.7.2 COM Express™ Connector Pin Assignment (continued)

Table 12: COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
A56	PCIE_TX4–	PCI Express differential transmit pair	O	
A57	GND	Ground	GND	
A58	PCIE_TX3+	PCI Express differential transmit pair	O	
A59	PCIE_TX3–	PCI Express differential transmit pair	O	
A60	GND (FIXED)	Ground	GND	
A61	PCIE_TX2+	PCI Express differential transmit pair	O	
A62	PCIE_TX2–	PCI Express differential transmit pair	O	
A63	GPI1/SD_DATA1	GPI1 / SDIO Data lines	I PU	GP or SD card
A64	PCIE_TX1+	PCI Express differential transmit pair	O	
A65	PCIE_TX1–	PCI Express differential transmit pair	O	
A66	GND	Ground	GND	
A67	GPI2/SD_DATA2	GPI2 / SDIO Data lines	I PU	GP or SD card
A68	PCIE_TX0+	PCI Express differential transmit pair	O	
A69	PCIE_TX0–	PCI Express differential transmit pair	O	
A70	GND (FIXED)	Ground	GND	
A71	LVDS_A0+	LVDS Channel A differential pair 0	O	Optional eDP
A72	LVDS_A0–	LVDS Channel A differential pair 0	O	Optional eDP
A73	LVDS_A1+	LVDS Channel A differential pair 1	O	Optional eDP
A74	LVDS_A1–	LVDS Channel A differential pair 1	O	Optional eDP
A75	LVDS_A2+	LVDS Channel A differential pair 2	O	Optional eDP
A76	LVDS_A2–	LVDS Channel A differential pair 2	O	Optional eDP
A77	LVDS_VDD_EN	LVDS eDP panel power enable	O	Optional eDP
A78	LVDS_A3+	LVDS Channel A differential pair 3	O	
A79	LVDS_A3–	LVDS Channel A differential pair 3	O	
A80	GND (FIXED)	Ground	GND	
A81	LVDS_A_CK+	LVDS Channel A differential clock	O	Optional eDP
A82	LVDS_A_CK–	LVDS Channel A differential clock	O	Optional eDP
A83	LVDS_I2C_CK	I^2C clock output for LVDS display	IO PU	Optional eDP
A84	LVDS_I2C_DAT	I^2C data line for LVDS display	IO PU	Optional eDP
A85	GPI3/SD_DATA3	GPI3 / SD_DATA3	I PU	GP or SD card
A86	RSVD	Reserved	NC	
A87	eDP_HPD	eDP (Hot Plug Detection)	I PD	Optional eDP
A88	PCIE_CLK_REF+	Reference clock output for all PCI Express lanes	O	
A89	PCIE_CLK_REF–	Reference clock output for all PCI Express lanes	O	
A90	GND (FIXED)	Ground	GND	
A91	SPI_POWER	Power supply for Carrier Board SPI	PWR	
A92	SPI_MISO	Data-in to Module from Carrier SPI	I PU	
A93	GPO0/SD_CLK	GPO0 / SDIO Clock	O PD	GP or SD card
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, transmit	O 3V3	Without protection
A99	SER0_RX	Serial port 0, receive	I 3V3	Without protection
A100	GND (FIXED)	Ground	GND	
A101	SER1_TX	Serial port 1, transmit	O 3V3	Without protection
A102	SER1_RX	Serial port 1, receive	I 3V3	Without protection
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	

3.7.2 COM Express™ Connector Pin Assignment (continued)

Table 12: 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	IO	LPC
B4	LPC_AD0/ESPI_IO_0	LPC multiplexed address, command and data bus	IO	LPC
B5	LPC_AD1/ESPI_IO_1	LPC multiplexed address, command and data bus	IO	LPC
B6	LPC_AD2/ESPI_IO_2	LPC multiplexed address, command and data bus	IO	LPC
B7	LPC_AD3/ESPI_IO_3	LPC multiplexed address, command and data bus	IO	LPC
B8	LPC_DRQ0#/ESPI_ALERT0#	LPC serial DMA request	IO	N/A
B9	LPC_DRQ1#/ESPI_ALERT1#	LPC serial DMA request	IO	N/A
B10	LPC_CLK/ESPI_CK	LPC clock output	O	LPC
B11	GND (FIXED)	Ground	GND	
B12	PWRBTN#	Power button input	I PU	TQ-flexiCFG
B13	SMB_CK	System Management Bus bidirectional clock line	IO PU	
B14	SMB_DAT	System Management Bus bidirectional data line	IO PU	
B15	SMB_ALERT#	System Management Bus Alert	I PU	
B16	SATA1_TX+	SATA differential transmit pair	O	
B17	SATA1_TX–	SATA differential transmit pair	O	
B18	SUS_STAT#/ESPI_RESET#	Indicates imminent suspend operation	O	LPC
B19	SATA1_RX+	SATA differential receive pair	I	
B20	SATA1_RX–	SATA differential receive pair	I	
B21	GND (FIXED)	Ground	GND	
B22	SATA3_TX+	SATA differential transmit pair	O	N/A
B23	SATA3_TX–	SATA differential transmit pair	O	N/A
B24	PWR_OK	Power OK from main power supply	I PU	TQ-flexiCFG
B25	SATA3_RX+	SATA differential receive pair	I	N/A
B26	SATA3_RX–	SATA differential receive pair	I	N/A
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 I^2C port clock output	O PU	TQ-flexiCFG
B34	I2C_DAT	General purpose I^2C port data I/O line	IO PU	TQ-flexiCFG
B35	THRM#	Input from carrier temperature sensor	I PU	
B36	USB7–	USB differential pair	IO	
B37	USB7+	USB differential pair	IO	
B38	USB_4_5_OC#	USB over-current sense, USB channels 4 and 5	I PU	
B39	USB5–	USB differential pair	IO	
B40	USB5+	USB differential pair	IO	
B41	GND (FIXED)	Ground	GND	
B42	USB3–	USB differential pair	IO	
B43	USB3+	USB differential pair	IO	
B44	USB_0_1_OC#	USB over-current sense, USB channels 0 and 1	I PU	
B45	USB1–	USB differential pair	IO	
B46	USB1+	USB differential pair	IO	
B47	ESPI_EN#	LPC/eSPI enable signal	I PU	LPC
B48	USB0_HOST_PRSNT	Module USB client may detect the presence of a USB host on USB0	I PU	TQ-flexiCFG
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 pair	I	
B53	PCIE_RX5–	PCI Express differential receive pair	I	
B54	GPO1/SD_CMD	GPO1 / SDIO Command	O PD	GP or SD card
B55	PCIE_RX4+	PCI Express differential receive pair	I	

3.7.2 COM Express™ Connector Pin Assignment (continued)

Table 12: COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
B56	PCIE_RX4–	PCI Express differential receive pair	I	
B57	GPO2 / SD_WP	GPO2 / SDIO Write Protect	O PD	GP or SD card
B58	PCIE_RX3+	PCI Express differential receive pair	I	
B59	PCIE_RX3–	PCI Express differential receive pair	I	
B60	GND (FIXED)	Ground	GND	
B61	PCIE_RX2+	PCI Express differential receive pair	I	
B62	PCIE_RX2–	PCI Express differential receive pair	I	
B63	GPO3/SD_CD#	GPO3 / SDIO Card Detect	O PD	GP or SD card
B64	PCIE_RX1+	PCI Express differential receive pair	I	
B65	PCIE_RX1–	PCI Express differential receive pair	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 pair	I	
B69	PCIE_RX0–	PCI Express differential receive pair	I	
B70	GND (FIXED)	Ground	GND	
B71	LVDS_B0+	LVDS Channel B differential pair 0	O	
B72	LVDS_B0–	LVDS Channel B differential pair 0	O	
B73	LVDS_B1+	LVDS Channel B differential pair 1	O	
B74	LVDS_B1–	LVDS Channel B differential pair 1	O	
B75	LVDS_B2+	LVDS Channel B differential pair 2	O	
B76	LVDS_B2–	LVDS Channel B differential pair 2	O	
B77	LVDS_B3+	LVDS Channel B differential pair 3	O	
B78	LVDS_B3–	LVDS Channel B differential pair 3	O	
B79	LVDS_BKLT_EN	LVDS panel backlight enable	O	Optional eDP
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 panel backlight brightness control	O	Optional eDP
B84	VCC_5V_SBY	Standby power input: +5.0 V nominal	PWR	
B85	VCC_5V_SBY	Standby power input: +5.0 V nominal	PWR	
B86	VCC_5V_SBY	Standby power input: +5.0 V nominal	PWR	
B87	VCC_5V_SBY	Standby power input: +5.0 V nominal	PWR	
B88	BIOS_DIS1#	Selection straps to determine the BIOS boot device	I PU	
B89	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	GND	

3.7.2 COM Express™ Connector Pin Assignment (continued)

Table 12: COM Express™ Connector Pin Assignment (continued)

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

3.7.2 COM Express™ Connector Pin Assignment (continued)

Table 12: COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
C56	PEG_RX1–	PCI Express differential receive pair	I	N/A
C57	TYPE1#	Type 1 Module indication (NC)	NC	
C58	PEG_RX2+	PCI Express differential receive pair	I	N/A
C59	PEG_RX2–	PCI Express differential receive pair	I	N/A
C60	GND (FIXED)	Ground	GND	
C61	PEG_RX3+	PCI Express differential receive pair	I	N/A
C62	PEG_RX3–	PCI Express differential receive pair	I	N/A
C63	RSVD	Reserved	NC	
C64	RSVD	Reserved	NC	
C65	PEG_RX4+	PCI Express differential receive pair	I	N/A
C66	PEG_RX4–	PCI Express differential receive pair	I	N/A
C67	RAPID_SHUTDOWN	Trigger for Rapid Shutdown. Must be driven to 5 V	I PD	
C68	PEG_RX5+	PCI Express differential receive pair	I	N/A
C69	PEG_RX5–	PCI Express differential receive pair	I	N/A
C70	GND (FIXED)	Ground	GND	
C71	PEG_RX6+	PCI Express differential receive pair	I	N/A
C72	PEG_RX6–	PCI Express differential receive pair	I	N/A
C73	GND	Ground	GND	
C74	PEG_RX7+	PCI Express differential receive pair	I	N/A
C75	PEG_RX7–	PCI Express differential receive pair	I	N/A
C76	GND	Ground	GND	
C77	RSVD	Reserved	N/C	
C78	PEG_RX8+	PCI Express differential receive pair	I	N/A
C79	PEG_RX8–	PCI Express differential receive pair	I	N/A
C80	GND (FIXED)	Ground	GND	
C81	PEG_RX9+	PCI Express differential receive pair	I	N/A
C82	PEG_RX9–	PCI Express differential receive pair	I	N/A
C83	RSVD	Reserved	NC	
C84	GND	Ground	GND	
C85	PEG_RX10+	PCI Express differential receive pair	I	N/A
C86	PEG_RX10–	PCI Express differential receive pair	I	N/A
C87	GND	Ground	GND	
C88	PEG_RX11+	PCI Express differential receive pair	I	N/A
C89	PEG_RX11–	PCI Express differential receive pair	I	N/A
C90	GND (FIXED)	Ground	GND	
C91	PEG_RX12+	PCI Express differential receive pair	I	N/A
C92	PEG_RX12–	PCI Express differential receive pair	I	N/A
C93	GND	Ground	GND	
C94	PEG_RX13+	PCI Express differential receive pair	I	N/A
C95	PEG_RX13–	PCI Express differential receive pair	I	N/A
C96	GND	Ground	GND	
C97	RSVD	Reserved	NC	
C98	PEG_RX14+	PCI Express differential receive pair	I	N/A
C99	PEG_RX14–	PCI Express differential receive pair	I	N/A
C100	GND (FIXED)	Ground	GND	
C101	PEG_RX15+	PCI Express differential receive pair	I	N/A
C102	PEG_RX15–	PCI Express differential receive pair	I	N/A
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	

3.7.2 COM Express™ Connector Pin Assignment (continued)

Table 12: COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
D1	GND (FIXED)	Ground	GND	
D2	GND	Ground	GND	
D3	USB_SSTX0–	SuperSpeedPlus USB3.1 differential transmit pair	O	
D4	USB_SSTX0+	SuperSpeedPlus USB3.1 differential transmit pair	O	
D5	GND	Ground	GND	
D6	USB_SSTX1–	SuperSpeedPlus USB3.1 differential transmit pair	O	
D7	USB_SSTX1+	SuperSpeedPlus USB3.1 differential transmit pair	O	
D8	GND	Ground	GND	
D9	USB_SSTX2–	SuperSpeedPlus USB3.1 differential transmit pair	O	
D10	USB_SSTX2+	SuperSpeedPlus USB3.1 differential transmit pair	O	
D11	GND (FIXED)	Ground	GND	
D12	USB_SSTX3–	SuperSpeedPlus USB3.1 differential transmit pair	O	
D13	USB_SSTX3+	SuperSpeedPlus USB3.1 differential transmit pair	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	RSVD	Reserved	NC	
D18	RSVD	Reserved	NC	
D19	PCIE_TX6+	PCI Express differential transmit pair	O	
D20	PCIE_TX6–	PCI Express differential transmit pair	O	
D21	GND (FIXED)	Ground	GND	
D22	PCIE_TX7+	PCI Express differential transmit pair	O	
D23	PCIE_TX7–	PCI Express differential transmit pair	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 pair 0	O	
D27	DDI1_PAIR0–	DDI1 DP / HDMI / DVI differential pair 0	O	
D28	RSVD	Reserved	NC	
D29	DDI1_PAIR1+	DDI1 DP / HDMI / DVI differential pair 1	O	
D30	DDI1_PAIR1–	DDI1 DP / HDMI / DVI differential pair 1	O	
D31	GND (FIXED)	Ground	GND	
D32	DDI1_PAIR2+	DDI1 DP / HDMI / DVI differential pair 2	O	
D33	DDI1_PAIR2–	DDI1 DP / HDMI / DVI differential pair 2	O	
D34	DDI1_DDC_AUX_SEL	Selects the function of DDI1_CTRLxAUX+/– Signals	I PD	
D35	RSVD	Reserved	NC	
D36	DDI1_PAIR3+	DDI1 DP / HDMI / DVI differential pair 3	O	
D37	DDI1_PAIR3–	DDI1 DP / HDMI / DVI differential pair 3	O	
D38	RSVD	Reserved	NC	
D39	DDI2_PAIR0+	DDI2 DP / HDMI / DVI differential pair 0	O	
D40	DDI2_PAIR0–	DDI2 DP / HDMI / DVI differential pair 0	O	
D41	GND (FIXED)	Ground	GND	
D42	DDI2_PAIR1+	DDI2 DP / HDMI / DVI differential pair 1	O	
D43	DDI2_PAIR1–	DDI2 DP / HDMI / DVI differential pair 1	O	
D44	DDI2_HPD	DDI2 Detection of Hot Plug	I PD	
D45	RSVD	Reserved	NC	
D46	DDI2_PAIR2+	DDI2 DP / HDMI / DVI differential pair 2	O	
D47	DDI2_PAIR2–	DDI2 DP / HDMI / DVI differential pair 2	O	
D48	RSVD	Reserved	NC	
D49	DDI2_PAIR3+	DDI2 DP / HDMI / DVI differential pair 3	O	
D50	DDI2_PAIR3–	DDI2 DP / HDMI / DVI differential pair 3	O	
D51	GND (FIXED)	Ground	GND	
D52	PEG_TX0+	PCI Express differential transmit pair	O	
D53	PEG_TX0–	PCI Express differential transmit pair	O	
D54	PEG_LANE_RV#	PCI Express Graphics lane reversal input strap	I	N/A
D55	PEG_TX1+	PCI Express differential transmit pair	O	N/A

3.7.2 COM Express™ Connector Pin Assignment (continued)

Table 12: COM Express™ Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Remark
D56	PEG_TX1–	PCI Express differential transmit pair	O	N/A
D57	TYPE2#	Type 2 Module indication (GND)	O	
D58	PEG_TX2+	PCI Express differential transmit pair	O	N/A
D59	PEG_TX2–	PCI Express differential transmit pair	O	N/A
D60	GND (FIXED)	Ground	GND	
D61	PEG_TX3+	PCI Express differential transmit pair	O	N/A
D62	PEG_TX3–	PCI Express differential transmit pair	O	N/A
D63	RSVD	Reserved	NC	
D64	RSVD	Reserved	NC	
D65	PEG_TX4+	PCI Express differential transmit pair	O	N/A
D66	PEG_TX4–	PCI Express differential transmit pair	O	N/A
D67	GND	Ground	GND	
D68	PEG_TX5+	PCI Express differential transmit pair	O	N/A
D69	PEG_TX5–	PCI Express differential transmit pair	O	N/A
D70	GND (FIXED)	Ground	GND	
D71	PEG_TX6+	PCI Express differential transmit pair	O	N/A
D72	PEG_TX6–	PCI Express differential transmit pair	O	N/A
D73	GND	Ground	GND	
D74	PEG_TX7+	PCI Express differential transmit pair	O	N/A
D75	PEG_TX7–	PCI Express differential transmit pair	O	N/A
D76	GND	Ground	GND	
D77	RSVD	Reserved	NC	
D78	PEG_TX8+	PCI Express differential transmit pair	O	N/A
D79	PEG_TX8–	PCI Express differential transmit pair	O	N/A
D80	GND (FIXED)	Ground	GND	
D81	PEG_TX9+	PCI Express differential transmit pair	O	N/A
D82	PEG_TX9–	PCI Express differential transmit pair	O	N/A
D83	RSVD	Reserved	NC	
D84	GND	Ground	GND	
D85	PEG_TX10+	PCI Express differential transmit pair	O	N/A
D86	PEG_TX10–	PCI Express differential transmit pair	O	N/A
D87	GND	Ground	GND	
D88	PEG_TX11+	PCI Express differential transmit pair	O	N/A
D89	PEG_TX11–	PCI Express differential transmit pair	O	N/A
D90	GND (FIXED)	Ground	GND	
D91	PEG_TX12+	PCI Express differential transmit pair	O	N/A
D92	PEG_TX12–	PCI Express differential transmit pair	O	N/A
D93	GND	Ground	GND	
D94	PEG_TX13+	PCI Express differential transmit pair	O	N/A
D95	PEG_TX13–	PCI Express differential transmit pair	O	N/A
D96	GND	Ground	GND	
D97	RSVD / M2_PE/SATA_DET	Reserved	I PU	TQ-flexiCFG
D98	PEG_TX14+	PCI Express differential transmit pair	O	N/A
D99	PEG_TX14–	PCI Express differential transmit pair	O	N/A
D100	GND (FIXED)	Ground	GND	
D101	PEG_TX15+	PCI Express differential transmit pair	O	N/A
D102	PEG_TX15–	PCI Express differential transmit pair	O	N/A
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 TQMx80UC has dimensions of 95 × 95 mm² (±0.2 mm).
The following illustration shows the TQMx80UC Three View Drawing.

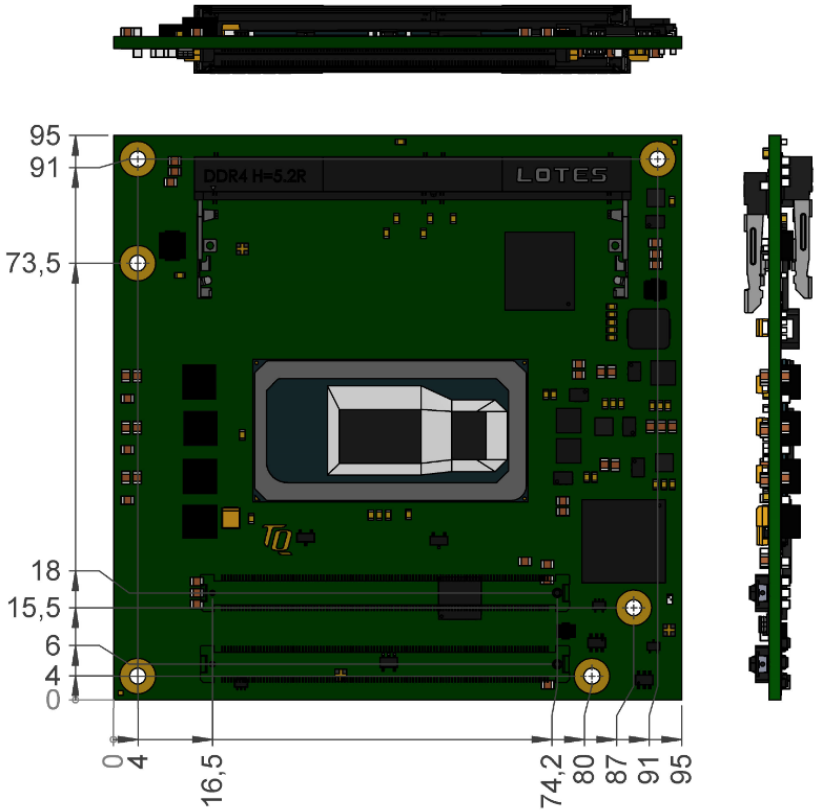


Illustration 3: TQMx80UC Three-View Drawing

The following illustration shows the TQMx80UC bottom view.

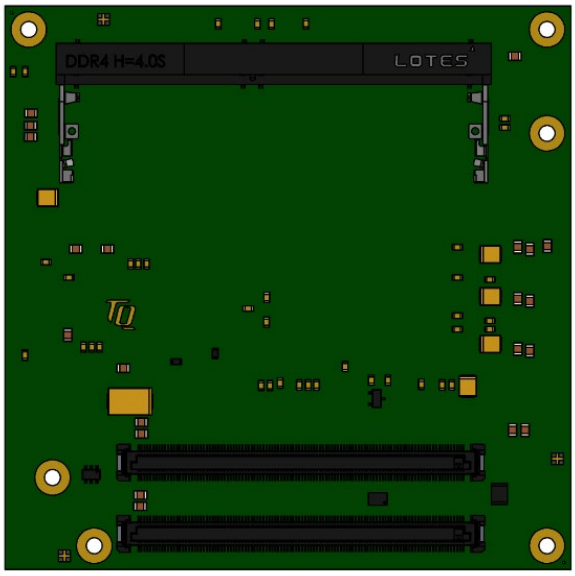


Illustration 4: TQMx80UC Bottom View Drawing

4.2 Component Placement

The following illustration shows the TQMx80UC component placement.

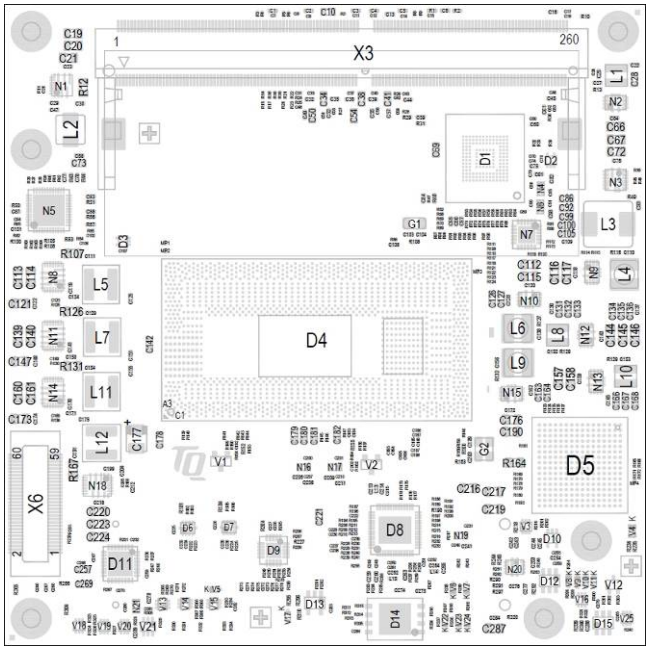


Illustration 5: TQMx80UC Component Placement Top

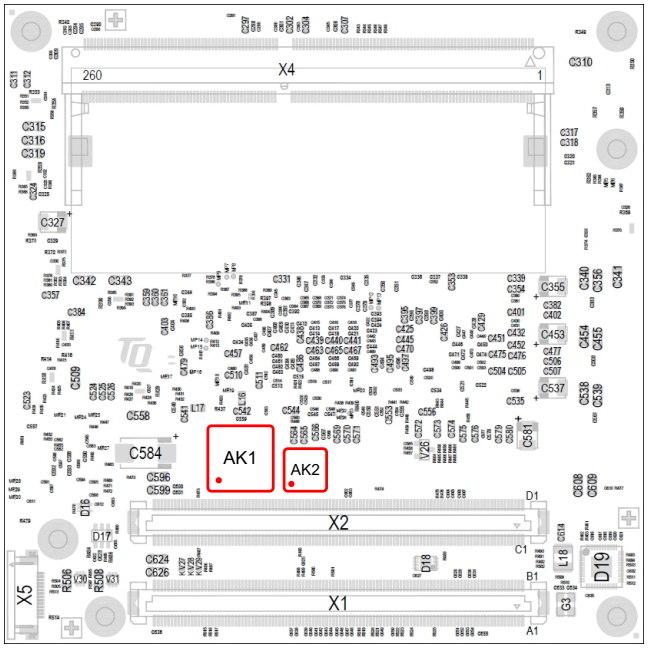


Illustration 6: TQMx80UC Component Placement Bottom

The labels on the TQMx80UC show the following information:

Table 13: Labels on TQMx80UC

Label	Text
AK1	MAC address, tests performed
AK2	TQMx80UC version and revision

4.3 Heat Spreader

A heat spreader "TQMx80UC-HSP" is available for the TQMx80UC.
The TQMx80UC 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 (TQMx80UC-HSP) for the TQMx80UC.

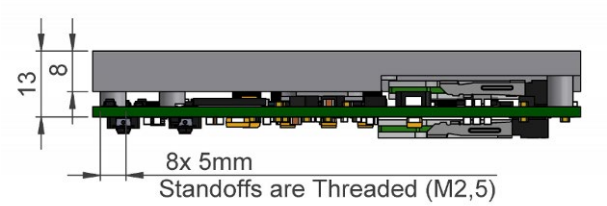


Illustration 7: TQMx80UC-HSP Heat Spreader

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 TQMx80UC 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 TQMx80UC. The heat spreader is thermally coupled to the processor and provides optimal heat transfer from the TQMx80UC 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 TQMx80UC 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 TQMx80UC 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 TQMx80UC 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 14: 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 TQMx80UC provides a System Management Bus (SMBus).
The following table shows the I²C address mapping for the COM Express™ SMBus port.

Table 15: I²C Address Mapping COM Express™ SMBus Port

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

5.1.3 Memory Mapping

The TQMx80UC supports the standard PC system memory and I/O memory map.

5.1.4 Interrupt Mapping

The TQMx80UC 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 TQMx80UC supports several Operating Systems:

- Microsoft® Windows® 10 (IoT) 2019 or later
- Linux (i.e. Ubuntu 18.04 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 TQMx80UC 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 TQMx80UC feature set.

Drivers for Graphics can be downloaded at this Intel® page:
https://downloadcenter.intel.com/product/128199/Graphics-for-8th-Generation-Intel-Processors

The Intel® Driver Update Utility is a tool that analyses the system drivers on your computer. It reports if any new drivers are available, and provides the download files for the driver updates so you can install them quickly and easily.
https://downloadcenter.intel.com/download/24345/Intel-Driver-Update-Utility

Drivers for the Intel® Gigabit Ethernet controller can be downloaded at this Intel® page:
https://downloadcenter.intel.com/download/26000/Intel-Network-Adapter-Driver-for-Windows-10

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 TQMx80UC uses a 64-bit uEFI BIOS with a legacy Compatibility Support Module (CSM).
This additional functionality enables the loading of a traditional OS or the use of a traditional OpROM.

To get access to 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.

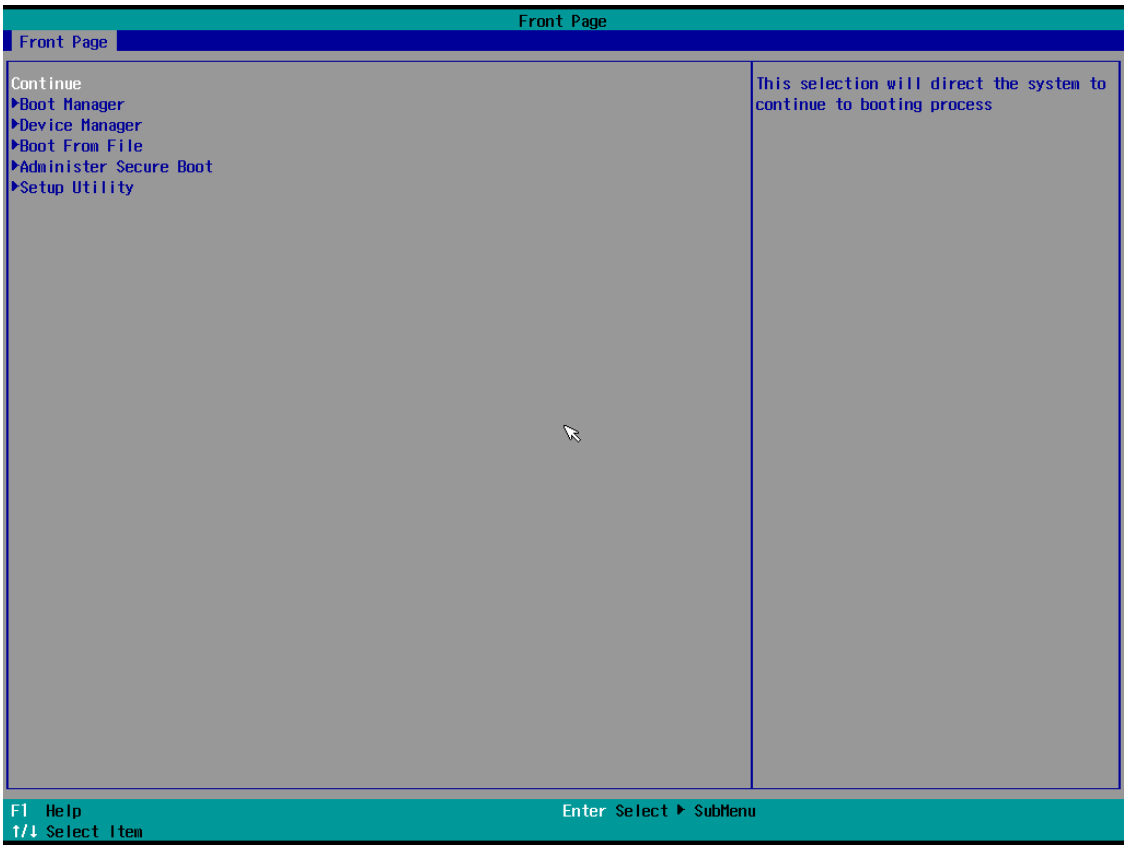


Illustration 8: InsydeH2O BIOS Front Page

6.1 Continue

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

6.2 Boot Manager

Choose between possible Boot Options. If system is in UEFI Boot Mode one Boot Option will be “Internal EFI Shell”.

6.3 Device Manager

6.3.1 SioTqmx86

Menu Item	Options	Description
GPIO/SD card configuration	GPIO interface / SD card interface	Configure the COM Express configuration as GPIO or SD card interface.
COME Lane 4-7 configuration	PCI Express / SATA / automatic via COME_RSVD_D97 signal	Configure the COM Express Lanes 4-7 PCI Express / SATA configuration for M.2 SSD device. Note: Configured as SATA system needs to make a reset while boot process which increases boot time.
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.
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 the LVDS dual/single mode in eDP-to-LVDS bridge.
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.

6.4 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: Advanced feature	
	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.
If the button successfully pressed can be seen by sentence “ESC is pressed. Go to boot options” shown below the boot logo.
On the splash screen that will appear, select “Setup Utility”.

The left frame of each menu page show option which can be configured whereas the right frame shows the corresponding help.

Key Legend:

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

6.6.1 Main

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

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

6.6.2 Advanced

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

Menu Item	Options	Description
Boot Configuration	See submenu	Configures settings for Boot Phase
Chipset Configuration	See submenu	Configure Platform Trust Technology
ACPI Table/Features Control	See submenu	Configure ACPI settings
CPU Configuration	See submenu	Configure CPU parameters
Power & Performance	See submenu	Configure Power Management Control
Memory Configuration	See submenu	Configure Memory parameters
System Agent (SA) Configuration	See submenu	Configure System Agent parameters like Graphic configuration
PCH-IO Configuration	See submenu	Configure PCH-IO parameters (PCI, SATA, USB, Audio, SCS, …)
PCH-FW Configuration	See submenu	Configure Management Engine (ME) parameters
Thermal Configuration	See submenu	Configure Digital Thermal sensor and ACPI T-States
SIO Hardware Monitor Nuvoton NCT78002Y	See submenu	Configure Fan Speed and Frequency. Shows Hardware Monitor Temperatures and Voltages.
Console Redirection	See submenu	Configure parameters of Console Redirection

6.6.2.1 Boot Configuration

Setup Utility ⇨ Advanced ⇨ Boot Configuration

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

6.6.2.2 Chipset Configuration

Setup Utility ⇨ Advanced ⇨ Chipset Configuration

Menu Item	Options	Description
Platform Trust Technology	Enabled / Disabled	Enable or disable Platform Trust Technology

6.6.2.3 ACPI Table/Features Control

Setup Utility ⇨ Advanced ⇨ ACPI Table/Features Control

Menu Item	Options	Description
ACPI Settings	See submenu	Set ACPI Configuration parameters
FACP – RTC S4 Wakeup	Enabled / Disabled	Value only for ACPI. Enables or disables 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 ⇨ ACPI Table/Features Control ⇨ ACPI Settings

Menu Item	Options	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 Operating Systems.
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	Enables or Disables ACPI S3 support
Native PCIE Enable	Enabled / Disabled	Bit – PCIe Native * Control 0 – ~ Hot Plug 1 – SHPC Native Hot Plug control 2 – ~ Power Management Events 3 – PCIe Advanced Error Reporting control 4 – PCIe Capability Structure control 5 – Latency Tolerance Reporting control
Native ASPM	Auto / Enabled / Disabled	Enabled – OS Controlled ASPM Disabled – BIOS Controlled ASPM
ACPI Debug	Enabled / Disabled	Open a memory buffer for storing debug strings. Re-enter SETUP after enabling to see the buffer address. Use method ADB6 to write strings to buffer.
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

6.6.2.4 CPU Configuration

Setup Utility ⇨ Advanced ⇨ CPU Configuration

Menu Item	Options	Description
C6DRAM	Enabled / Disabled	Enable or Disable moving of DRAM contents to PRM memory when CPU is in C6 state.
CPU Flex Ratio Override	Enabled / Disabled	Enable or Disable CPU Flex Ratio Programming.
CPU Flex Ratio Settings	0 – X	This value must be between Max Efficiency Ratio (LFM) and Maximum non-turbo ratio set by Hardware (HFM). This option will be greyed if CPU Flex Ration Override is disabled.
Hardware Prefetcher	Enabled / Disabled	To turn on/off the MLC streamer prefetcher.
Adjacent Cache Line Prefetch	Enabled / Disabled	To turn on/off prefetching of adjacent cache lines.
Intel (VMX) Virtualization Technology	Enabled / Disabled	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Active Processor Cores	All / 1 / 2 / 3	Number of cores to enable in each processor package.
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.
Intel Trusted Execution Technology	Enabled / Disabled	Enables utilization of additional hardware capabilities provided by Intel® Trusted Execution Technology. Changes require a full power cycle to take effect.
Alias Check Request	Enabled / Disabled	Enables Txt Alias Checking capability. Changes require full Txt capability before it will take effect. It is a one-time only change, next reboot will be reset. This option will be greyed if Intel Trusted Execution Technology is Disabled.
DPR Memory Size (MB)	0 – 255	Reserve DPR memory size (0 – 255) MB. This option will be greyed if Intel Trusted Execution Technology is Disabled.
Reset AUX Content	Yes / no	Reset TPM Aux content. Txt may not functional after AUX content gets reset. This option will be greyed out if Intel Trusted Execution Technology is Enabled.

6.6.2.5 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.
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	Information page	View Turbo Options.
Config TDP Configurations	See submenu	Configure TDP Options.
C states	Enabled / Disabled	Enable or Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
Enhanced C-states	Enabled / Disabled	Enable or Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State. This option will be hidden if C states is Disabled.
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.
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.

6.6.2.5 Power & Performance (continued)

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

Menu Item	Options	Description
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.
CTDP BIOS control	Enabled / Disabled	Enables CTDP control via runtime ACPI BIOS methods. This "BIOS only" feature does not require EC or driver support. This option is hidden if Configurable TDP Lock is Enabled.
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 ⇨ 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.

6.6.2.6 Memory Configuration

Setup Utility ⇨ Advanced ⇨ Memory Configuration

Menu Item	Options	Description
REFRESH_2X_MODE	Disabled / 1 – Enabled for WARM or HOT / 2 – Enabled HOT only	0 – Disabled 1 – iMC enables 2 × Ref when Warm and Hot 2 – iMC enables 2 × Ref when Hot
Row Hammer Solution	Hardware RHP / 2 × Refresh	Type of method used to prevent Row Hammer.
Channel A DIMM Control	Enabled both DIMMs / Disable DIMM0 / Disable DIMM1 / Disable both DIMMs	Channel A DIMM Control Support – Enable or Disable DIMMs on Channel A.
Channel B DIMM Control	Enabled both DIMMs / Disable DIMM0 / Disable DIMM1 / Disable both DIMMs	Channel B DIMM Control Support – Enable or Disable DIMMs on Channel B.

6.6.2.7 System Agent (SA) Configuration

Setup Utility ⇨ Advanced ⇨ System Agent (SA) Configuration

Menu Item	Options	Description
Graphics Configuration	See submenu	Configure some graphical options.
Stop Grant Configuration	Auto / Manual	Automatic/Manual stop grant configuration
VT-d	Enabled / Disabled	VT-d capability.
CHAP Device (B0:D7:F0)	Enabled / Disabled	Enable or Disable SA CHAP Device.
Thermal Device (B0:D4:F0)	Enabled / Disabled	Enable or Disable SA Thermal 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.
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.
X2APIC Opt Out	Enabled / Disabled	Enable or Disable X2APIC_OPT_OUT bit.
IPU Device (B0:D5:F0)	Enabled / Disabled	Enable or Disable SA IPU Device.

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

Menu Item	Options	Description
Graphics Turbo IMON Current	14 – 31	Graphics turbo IMON value.
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 / Disabled / Enabled	Keep IGFX enabled based on the setup options.
GTT Size	2 MB / 4 MB / 8 MB	Select the GTT Size.
Aperture Size	128 MB / 256 MB / 512 MB / 1024 MB / 2048 MB	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	Enable or Disable PSMI support.
DVMT Pre-Allocated	0 M – 60 M	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the internal Graphics Device.
DVMT Total Gfx Mem	128 M / 256 M / MAX	Select DVMT5.0 Total Graphic Memory size used by the internal Graphics Device.
Intel Graphics Pei Display Peim	Enabled / Disabled	Enable or Disable Pei (Pre-EFI Initialization; early) Display.
VDD Enable	Enabled / Disabled	Enable or Disable forcing of VDD in the BIOS.
PM Support	Enabled / Disabled	Enable or Disable PM Support.
PAVP Enable	Enabled / Disabled	Enable or Disable PAVP (Protected Audio Video Path).
Cdynmax Clamping Enable	Enabled / Disabled	Enable or Disable Cdynmax Clamping Enable.
Cd Clock Frequency	337.5 MHz / 450 MHz / 540 MHz / 675 MHz	Select the highest Cd Clock frequency supported by the platform.
Skip CD Clock Init in S3 resume	Enabled / Disabled	Enabled: Skip Full CD clock initialization. Disabled: Initialize the full CD clock in S3 resume due to GOP absent.
IUER Button Enable	Enabled / Disabled	Enable or Disable IUER Button Functionality.
LCD Control	See submenu	LCD Control options. Note: This menu is only visible in 'Dual Boot Mode' or 'Legacy Mode' because these options does not affect GOP (Graphical Output Protocol) used in UEFI Boot Mode.

6.6.2.7 System Agent (SA) Configuration (continued)

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

If "Boot Type" is set to "Dual Boot Type" or "Legacy Boot Type".

Menu Item	Options	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. No eDP: VBIOS does not enable eDP. eDP Port-A: LFP Driven by Int-DisplayPort encoder from Port-A.
Panel Color Depth	18 Bit / 24 Bit	Select the LFP Panel Color Depth.
Backlight Brightness	0 – 255	Set VBIOS Brightness. Range: 0 – 255

6.6.2.8 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.
SCS Configuration	See submenu	Storage and Communication Subsystem (SCS) Configuration settings.
PCH LAN Controller	Enabled / Disabled	Enable or Disable on-board NIC.
LAN Wake From DeepSx	Enabled / Disabled	Wake from DeepSx by the assertion of LAN_WAKE# pin.
Wake on LAN Enable	Enabled / Disabled	Enable or Disable integrated LAN to wake the system.
SLP_LAN# Low on DC Power	Enabled / Disabled	Enable or Disable SLP_LAN# Low on DC Power.
Disqualify GPE Disconnect And ModPhy PG	Enabled / Disabled	Enable or Disable the Disqualify GBE Disconnect And ModPhy PG bits.
EFI Network	On-board NIC / WiFi / On-board NIC & WiFi / Disabled	Enable or Disable EFI Network support for on-board LAN or WiFi module.
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).
PCIe PII SSC	Auto / 0.0% – 2.0%	PCIe PII SSC percentage. Auto – Keep HW default. No BIOS override.
Flash Protection Range Registers (FPRR)	Enabled / Disabled	Enable Flash Protection Range Registers.
RST Driver Select	Auto / Force Locked RST / Force Unlocked RST	Force locked/unlocked RST Pre-OS Driver to load.

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

Menu Item	Options	Description
DMI Link ASPM Control	Disabled / L0s / L1 / L0xL1 / Auto	The control of Active State Power Management of the DMI Link.
PCI Express Root Port X	See submenu	Configuration of the corresponding PCI Express Root Port X.

6.6.2.8 PCH-IO Configuration (continued)

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

Menu Item	Options	Description
PCI Express Root Port X	Enabled / Disabled	Control the PCI Express Root Port.
Topology	Board specific / Unknown / x1 / x4 / SATA Express / M2	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2.
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.
ASPM4	Disabled / L0s / L1 / L0sL1 / Auto	Automatically enable ASPM based on reported capabilities and known issues.
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.
UPTP	0 – 9	Upstream Port Transmitter Preset.
UDTP	0 – 9	Downstream Port Transmitter Preset.
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.
CTO	Enabled / Disabled	PCI Express Completion Timer TO 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	0 – 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.

6.6.2.8 PCH-IO Configuration (continued)

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.
Software Feature Mask Configuration	See submenu	RST Legacy OROM/RST UEFI driver will refer to the SWFM configuration to enable/disable the storage features.
Port X	Enabled / Disabled	Enable or Disable SATA Port.
Hot Plug	Enabled / Disabled	Designates this port as Hot Pluggable.
External	Enabled / Disabled	Marks this port as external.
Spin Up Device	Enabled / Disabled	If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive / Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.
Topology	Unknown / ISATA / Direct Connect / Flex / M2	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2.
DITO Configuration	Enabled / Disabled	Enable or Disable DITO Configuration.
DITO Value	0 – 999	DITO Value. Note: This option is only configurable if “DITO Configuration” is Enabled.
DM Value	0 – 15	DM Value. Note: This option is only configurable if “DITO Configuration” is Enabled.

Setup Utility ⇨ Advanced ⇨ PCH-IO Configuration ⇨ SATA and RST Configuration ⇨ Software Feature Mask Configuration

Menu Item	Options	Description
HDD Unlock	Enabled / Disabled	If enabled, indicates that the HDD password unlock in the OS is enabled.
LED Locate	Enabled / Disabled	If enabled, indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.

6.6.2.8 PCH-IO Configuration (continued)

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

Menu Item	Options	Description
xDCI Support	Enabled / Disabled	Enable or Disable xDCI (USB OTG Device).
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	Disable / Select Per-Pin	Selectively Enable or Disable the corresponding USB port from reporting a Device Connection to the controller.
USB 3.1/2.0 Physical Connector #X	Enabled / Disabled	Enable or Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS. Note: This option(s) are hidden if 'USB Port Disable Override' is Disabled.

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.

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

Menu Item	Options	Description
eMMC 5.0 Controller	Enabled / Disabled	Enable or Disable SCS eMMC 5.0 Controller.
SD card 3.0 Controller	Enabled / Disabled	Enable or Disable SCS SDMC 3.0 Controller.

6.6.2.9 PCH-FW Configuration

Setup Utility ⇨ Advanced ⇨ PCH-FW Configuration

Menu Item	Options	Description
Firmware Update Configuration	See submenu	Prepare ME FW for Update.

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

Menu Item	Options	Description
Me FW Image Re-Flash	Enabled / Disabled	Enable or Disable Me FW Image Re-Flash function. This option is needed when updating the ME FW. Note: This option is only valid for next boot.

6.6.2.10 Thermal Configuration

Setup Utility ⇨ Advanced ⇨ Thermal Configuration

Menu Item	Options	Description
CPU Thermal Configuration	See submenu	CPU Thermal Configuration options.

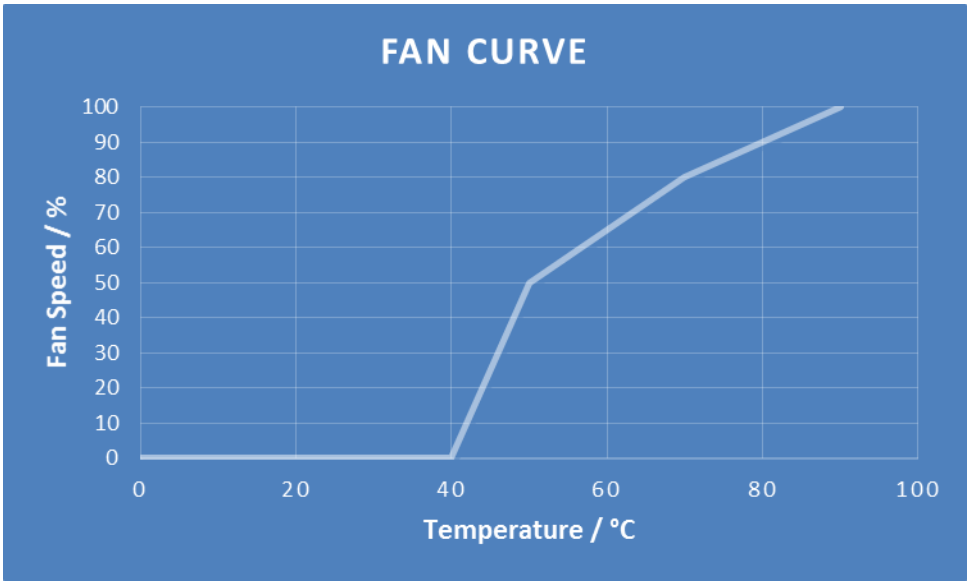
Setup Utility ⇨ Advanced ⇨ Thermal Configuration ⇨ CPU Thermal Configuration

Menu Item	Options	Description
DTS SMM	Enabled / Disabled / Critical Temp Reporting (Out of Spec)	Disabled: ACPI thermal management uses EC reported temperature values. Enabled: ACPI thermal management uses DTS SMM mechanism to obtain CPU temperature values. Out of Spec: ACPI Thermal Management uses EC reported temperature values and DTS SMM is used to handle Out of Spec condition.
ACPI T-States	[ ] / [X]	Enable or Disable ACPI T-States.

6.6.2.11 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.



6.6.2.12 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 Post	Yes / No	Console Redirection continue works after POST time.
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
AutoRefresh	Enabled / Disabled	When feature enable, screen will be auto refresh once after detect remote terminal was connected.
COM_X (COMA/B)	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.
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.

6.6.3 Security

For TPM 2.x:

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
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.
Wake on S5 Time	[XX:XX:XX]	This is the help for the hour, minute, second field. Valid range is from 0 to 23, 0 to 59 and 0 to 59. Increase and reduce by +/–. Note: This option is only visible if 'Auto Wake on S5' is set on 'By Every Day' or 'By Day of Month'.
Day of Month	[X]	This is the help for the day field. Valid range is from 1 to 31. (Error checking will be done against month/day/year combinations that are not supported). Increase and reduce by +/–. Note: This option is only visible if 'Auto Wake on S5' is set on 'By Day of Month'.

6.6.5 Boot

Menu Item	Options	Description
Boot Type	Dual Boot Type / Legacy Boot Type / UEFI Boot Type	Select boot type to Dual type, Legacy type or UEFI type. Note: Operating systems installed in UEFI only will boot in UEFI or Dual boot type, not in Legacy. Also the other way around when an OS is installed in Legacy it will not boot in UEFI type.
Quick Boot	Enabled / Disabled	Allow InsydeH2O to skip certain tests while booting. This will decrease the time needed to boot the system.
Quite Boot	Enabled / Disabled	Enable or disable booting in Text mode. No textual outputs are given while booting if this option is disabled.
Network Stack	Enabled / Disabled	Enable or disable Network stack Support: Windows 8 BitLocker Unlock UEFI IPv4/IPv6 PXE Legacy PXE OPROM Note: This option will grey-out the PXE Boot capability option.
PXE Boot capability	Disabled / UEFI : IPv4 / UEFI : IPv6 / UEFI : IPv4/IPv6	Disabled: Support Network Stack UEFI PXE: IPv4/IPv6 Legacy: Legacy PXE OPROM only 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.
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.
EFI Device First	Enabled / Disabled	Determine EFI device first or legacy device first. Enabled: EFI Device first. Disabled: Legacy Device first.
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 / Legacy	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	Options	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 TQMx80UC.
Please read the entire instruction before beginning the BIOS update.
By disregarding the information you can destroy the uEFI BIOS on the TQMx80UC.
This document will guide to update the uEFI BIOS on the TQMx80UC by using the Insyde Flash Firmware Tools.
Please contact support@tq-group.com for more information to the latest uEFI BIOS version for the TQMx80UC.

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 Step 1: Preparing USB Stick

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

- H2OFFT-Sx64.efi (Flash Firmware Tool from Insyde for update via UEFI Shell)
  - Be sure to have H2OFFT Version 200.00.00.02 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

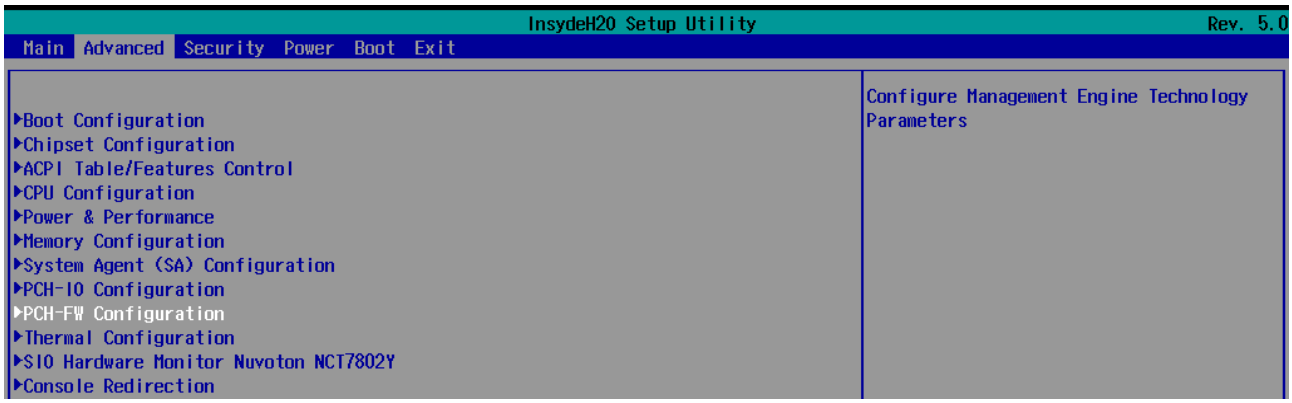


Illustration 9: PCH-FW Configuration menu

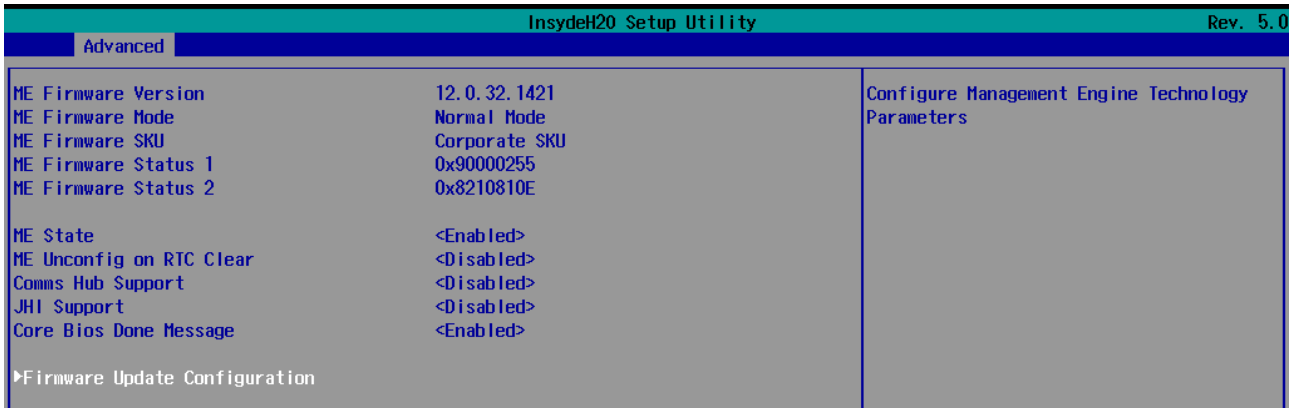


Illustration 10: Firmware Update configuration menu

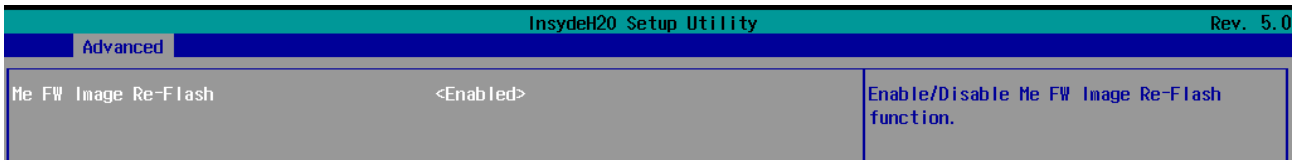


Illustration 11: ME FW Image Re-Flash option

Note: Unexpected long boot time	
	The boot time after setting the option mentioned above depends on the processor core. A Celeron™ CPU may require up to two minutes.

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

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

Setup Utility ⇨ Advanced ⇨ 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.

7.3 Step 3a: Updating uEFI BIOS via EFI Shell

Plug the USB stick into the board you want to update the uEFI BIOS, and turn on the board. The board will boot and go to the internal EFI shell.

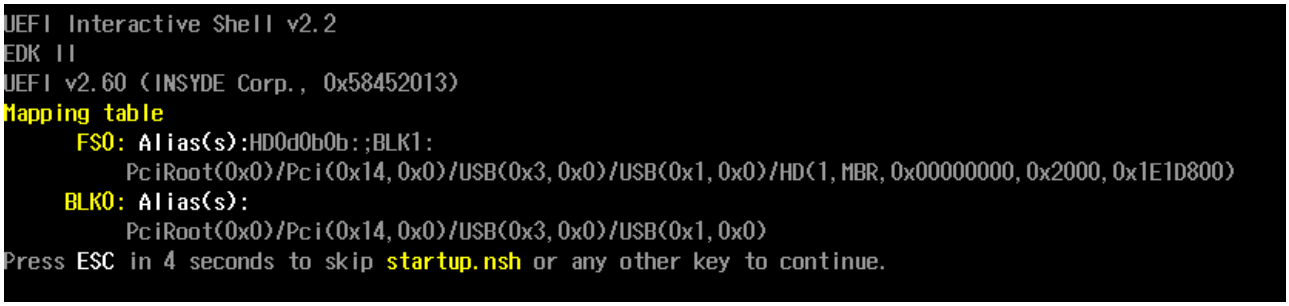


Illustration 12: EFI Shell

The device named “fs0” should be visible, this is the USB stick.
Move operating directory to USB drive with “fs0:”
Then, enter into the BIOS folder (e.g. “`cd tqmx80`”) to execute the Insyde BIOS update tool:

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

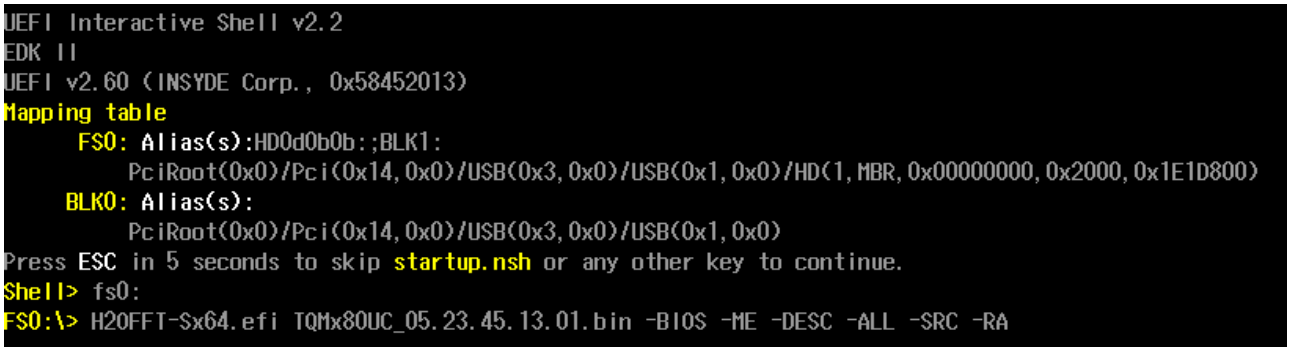


Illustration 13: EFI Shell uEFI BIOS Update

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

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

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

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

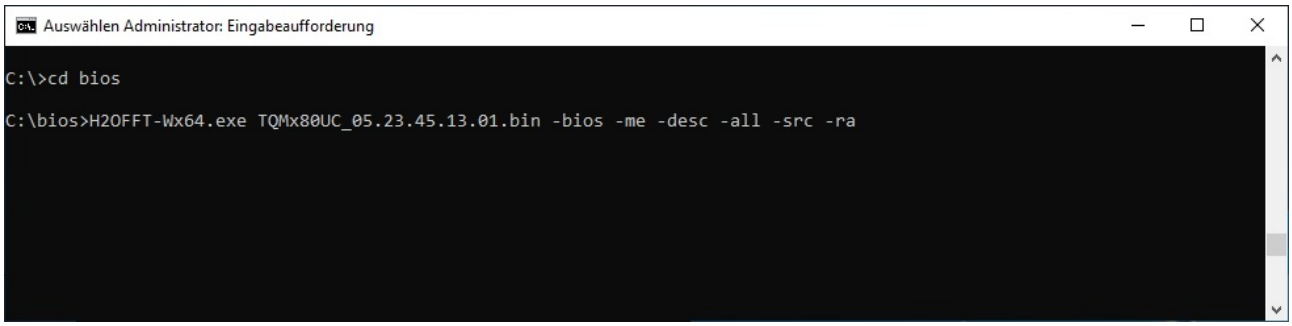


Illustration 14: Windows 10 64-bit BIOS folder

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

Note: Delayed BIOS update	
	The start of updating the BIOS may need a longer time (up to 2 or 3 minutes). The initializing information of the current and the new BIOS will be shown immediately, whereas the “Updating Block at …” requires more time.

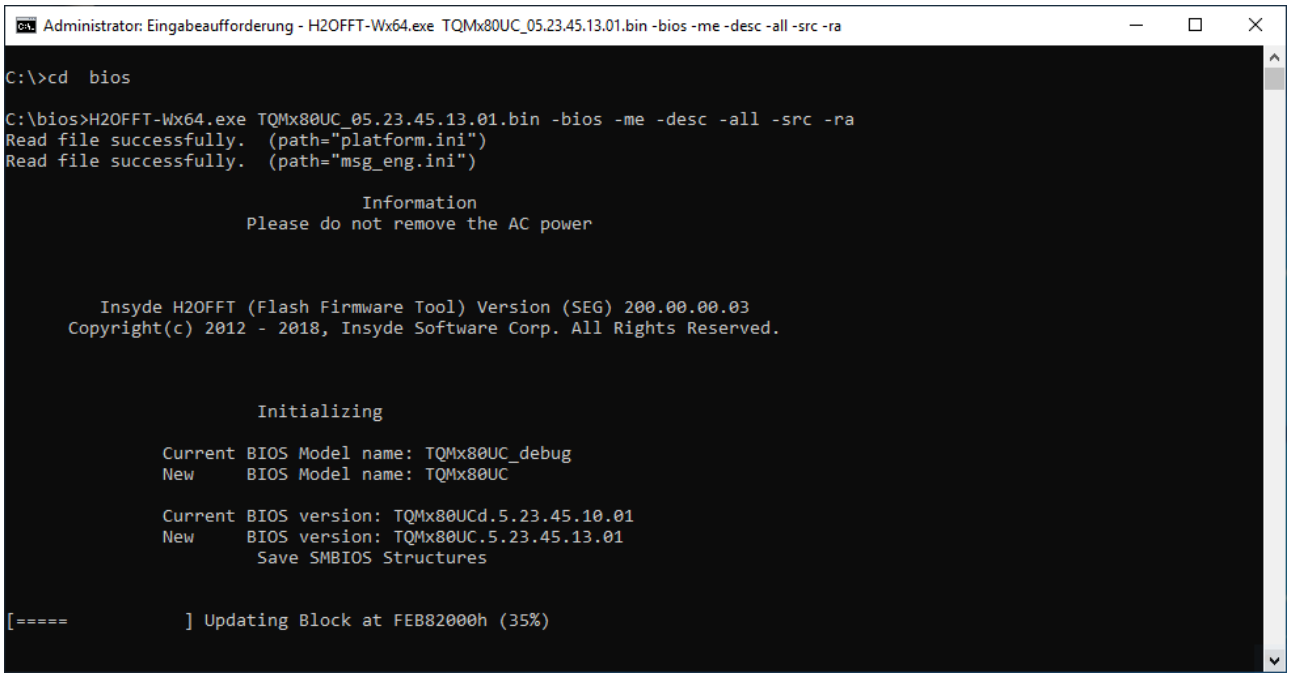


Illustration 15: Windows 10 64-bit BIOS update

7.5 Step 4: BIOS update check on the TQMx80UC Module

After an uEFI BIOS update, the new uEFI BIOS completely configures the TQMx80UC hardware.
This may result in several reboots and the first boot may take significantly longer (up to two minutes).
The TQMx80UC includes a dual-colour Debug LED providing boot and uEFI BIOS information.
When the green LED blinks, the uEFI BIOS is booting. When the green LED is lit, the uEFI BIOS boot is finished.

Illustration 16: TQMx80UC green Debug LED

After the uEFI BIOS has been flashed completely, perform a power cycle to check whether the uEFI BIOS has been flashed successfully. The BIOS Main menu includes board and hardware information and shows the installed BIOS version.

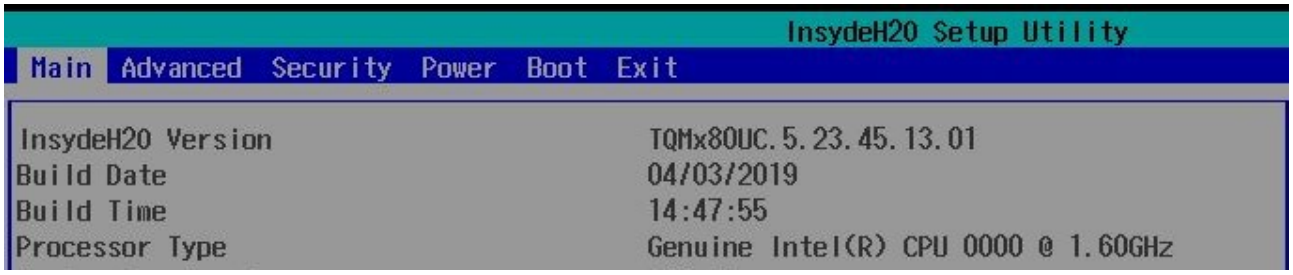


Illustration 17: EFI BIOS Main Menu

8. SAFETY REQUIREMENTS AND PROTECTIVE REGULATIONS

8.1 EMC

The TQMx80UC 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 TQMx80UC.

8.3 Shock & Vibration

The TQMx80UC 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 344,858 h, Ground Benign, @ +40 °C.

8.5.1 RoHS

The TQMx80UC 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 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 16: 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 16: 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 17: Further Applicable Documents and Links

No.	Name	Rev., Date	Company
(1)	8th Generation Intel® Core™ U Mobile processor series Product Brief	–	Intel
(2)	8th Generation Intel® Core™ UE Embedded processor series Product Brief	–	Intel
(3)	PICMG® COM Express™ Module Base Specification	Rev. 3.0, March 31, 2017	PICMG
(4)	PICMG® COM Express™ Carrier Design Guide	Rev. 2.0, Dec. 6, 2013	PICMG
(5)	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