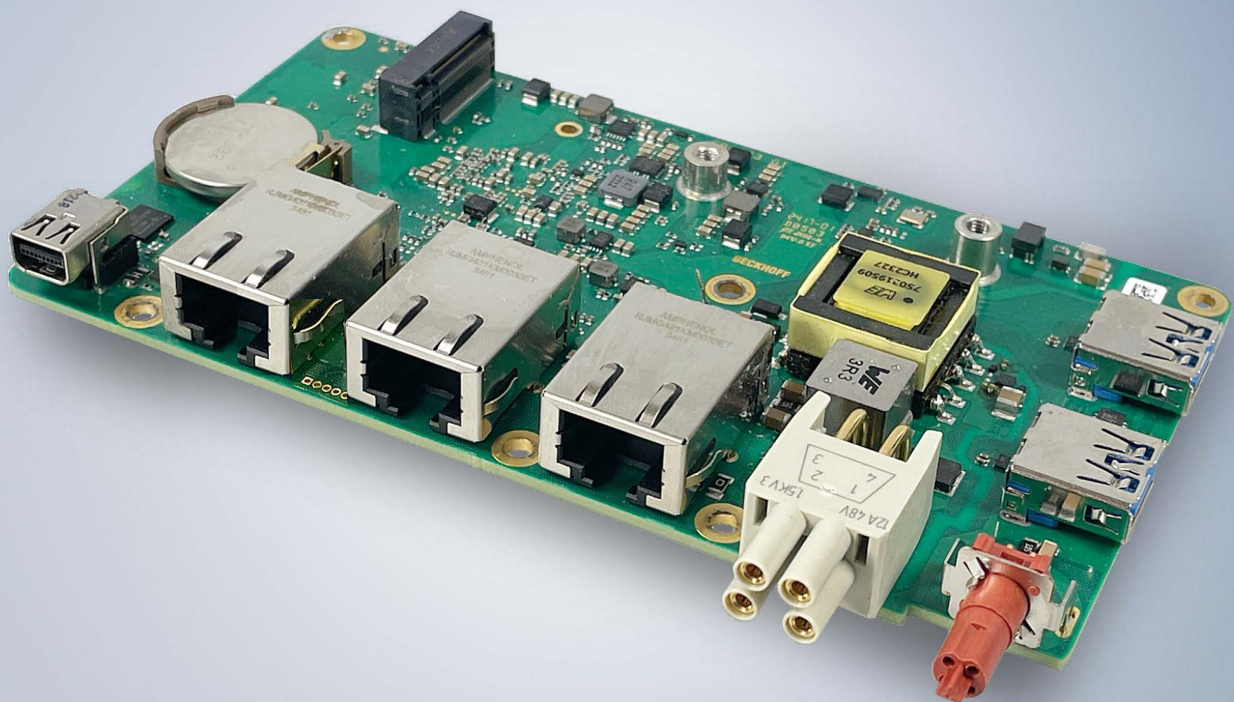


Operating Manual | EN

CB8283

Computerboard



1	Documentation issue status	5
2	Notes on the documentation	6
3	Safety instructions	7
4	Notes on information security	9
5	Overview	10
5.1	Properties	10
5.2	List of features	11
5.3	Specifications and documents	12
6	Detailed description	13
6.1	Power supply	13
6.2	CPU	13
6.3	Memory	13
6.4	M.2 socket	13
7	Interfaces	14
7.1	Note on the use of cables	14
7.2	Interface overview	15
7.3	List of interfaces	15
7.4	External interfaces	16
7.4.1	USB 3.2 IP65/67 (P1103, P1101)	16
7.4.2	EtherCAT P IP65/67 (P1106)	17
7.4.3	Power connection IP65/67 (P1107)	18
7.4.4	LAN IP65/67 (P1100, P1102, P1104)	19
7.4.5	Mini DisplayPort IP65/67 (P1005)	20
7.5	Internal interfaces	21
7.5.1	M.2 2242/2280k Key B (P1000)	21
7.5.2	Battery (BT500)	23
8	BIOS	24
8.1	Using the setup	24
8.2	Main CB8283	25
8.3	Advanced	26
8.3.1	RC ACPI settings	27
8.3.2	CPU Configuration	28
8.3.3	Trusted Computing	30
8.3.4	ACPI Settings	31
8.3.5	Hardware Monitor	31
8.3.6	Acoustic Management Configuration	32
8.3.7	PCI Subsystem Settings	33
8.3.8	USB Configuration	34
8.3.9	Network Stack Configuration Disabled	35
8.3.10	Network Stack Configuration Enabled	35
8.3.11	Power Controller Options	36
8.3.12	NVMe Configuration	37

8.3.13	RAM Disk Configuration.....	37
8.3.14	Intel Ethernet Controller I226-IT.....	39
8.3.15	Intel Ethernet Controller I226-IT.....	40
8.3.16	Intel Ethernet Controller I226-IT.....	41
8.3.17	User Password Management.....	42
8.3.18	Driver Health	42
8.4	Chipset.....	43
8.4.1	System Agent (SA) Configuration	43
8.4.2	PCH-IO Configuration	48
8.5	Security	72
8.5.1	Secure Boot	73
8.6	Boot.....	81
8.6.1	Advanced Fixed Boot Order Parameters	82
8.7	Save & Exit.....	83
8.8	BIOS update.....	84
9	LEDs	85
9.1	LED: UPS-OCT	85
9.2	LED: PWR	86
9.3	LED: SATA.....	86
9.4	LED: TwinCAT	86
9.5	LED: LAN 1 - LAN 3	87
9.6	EtherCAT LEDs.....	87
9.7	Power supply LED board	87
10	Mechanical drawing	88
10.1	Printed circuit board: dimensions and holes	88
11	Technical data	89
11.1	Electrical data.....	89
11.2	Environmental conditions	89
11.3	Thermal specifications	90
12	Appendix I: Post Codes	91
13	Appendix II: Resources	92
13.1	Interrupt.....	92
13.2	PCI-Devices	92
13.3	SMB-Devices	93
14	Support and Service	94

1 Documentation issue status

Version	Modifications
0.1	First preliminary version G1
1.0	First release, version G1

2 Notes on the documentation

This description is intended exclusively for trained specialists in control and automation technology who are familiar with the applicable national standards.

For installation and commissioning of the components, it is absolutely necessary to observe the documentation and the following notes and explanations.

It is the duty of the responsible staff to use the documentation published at the respective time of each installation and commissioning.

The responsible staff must ensure that the application or use of the products described satisfy all the requirements for safety, including all the relevant laws, regulations, guidelines and standards.

Origin of the document

This documentation was originally written in German. All other languages are derived from the German original.

Disclaimer

The documentation has been prepared with care. The products described are, however, constantly under development.

We reserve the right to revise and change the documentation at any time and without notice.

No claims for the modification of products that have already been supplied may be made on the basis of the data, diagrams, and descriptions in this documentation.

Trademarks

Beckhoff®, TwinCAT®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® and XPlanar® are registered and licensed trademarks of Beckhoff Automation GmbH.

Other designations used in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owners.

Patents

The EtherCAT Technology is covered, including but not limited to the following patent applications and patents:

EP1590927, EP1789857, EP1456722, EP2137893, DE102015105702

and similar applications and registrations in several other countries.

EtherCAT 

EtherCAT® is registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany

Copyright

© Beckhoff Automation GmbH & Co. KG, Germany.

The distribution and reproduction of this document as well as the use and communication of its contents without express authorization are prohibited.

Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.

3 Safety instructions

Safety regulations

Please observe the following safety instructions and explanations!
Product-specific safety instructions can be found on following pages or in the mounting, wiring, commissioning areas, etc.

Exclusion of liability

All of the components are supplied in specific hardware and software configurations depending on the application requirements. Modifications to hardware or software configurations other than those described in the documentation are not permitted, and nullify the liability of Beckhoff Automation GmbH & Co. KG.

Personnel qualification

This description is only intended for trained specialists in control, automation, and drive technology who are familiar with the applicable national standards.

Description of symbols

In this documentation the following symbols are used with an accompanying safety instruction or note. The safety instructions must be read carefully and followed without fail!

DANGER

Serious risk of injury!

Failure to follow the safety instructions associated with this symbol directly endangers human life and health!

WARNING

Risk of injury!

Failure to follow the safety instructions associated with this symbol endangers human life and health!

CAUTION

Personal injuries!

Failure to follow the safety instructions associated with this symbol can lead to physical injuries!

NOTICE

Damage to the environment or devices

Failure to follow the instructions associated with this symbol can lead to damage to the environment or equipment.

Tip or pointer



This symbol indicates information that contributes to better understanding.

UL note



This symbol indicates important information regarding UL approval.

Intended use

The CB8283 Computer Board was designed and developed exclusively for configuration in automation processes. To that end the board is equipped with external interfaces in order to acquire or output digital or analog signals or forward them to higher-level components.

The computer board has been developed for an IP65 working environment. It offers full protection against contact (dust-tight) and against water jets (nozzle) from any angle.

The specified limits for electrical and technical data must be adhered to.

Any other use is regarded as inappropriate.

4 Notes on information security

The products of Beckhoff Automation GmbH & Co. KG (Beckhoff), insofar as they can be accessed online, are equipped with security functions that support the secure operation of plants, systems, machines and networks. Despite the security functions, the creation, implementation and constant updating of a holistic security concept for the operation are necessary to protect the respective plant, system, machine and networks against cyber threats. The products sold by Beckhoff are only part of the overall security concept. The customer is responsible for preventing unauthorized access by third parties to its equipment, systems, machines and networks. The latter should be connected to the corporate network or the Internet only if appropriate protective measures have been set up.

In addition, the recommendations from Beckhoff regarding appropriate protective measures should be observed. Further information regarding information security and industrial security can be found in our <https://www.beckhoff.com/secguide>.

Beckhoff products and solutions undergo continuous further development. This also applies to security functions. In light of this continuous further development, Beckhoff expressly recommends that the products are kept up to date at all times and that updates are installed for the products once they have been made available. Using outdated or unsupported product versions can increase the risk of cyber threats.

To stay informed about information security for Beckhoff products, subscribe to the RSS feed at <https://www.beckhoff.com/secinfo>.

5 Overview

5.1 Properties

The CB8283 is designed as a compact, high-performance IP65/67 motherboard. On account of its wide variety of interfaces (3 x LAN 2.5 GB, 2 x USB3.2, mini DisplayPort, EtherCAT P), 40 GB M.2 SSD with 3D flash and integrated Intel Atom[®] CPU (quad-core at most) with universal multi-core support for TwinCAT 3, this motherboard can be used in robust industrial PCs for simultaneous, high-performance automation, visualization and communication under hard real-time conditions: from the classic machine controller to modern Industry 4.0 concepts as an edge device.

The integrated EtherCAT P connection enables you to connect actuators/sensors directly via IP67-protected EtherCAT P Box modules.

The compact format of the CB8283 offers the full functionality of a motherboard for space-saving and freely mountable industrial PC hardware and advanced Industry 4.0 concepts.

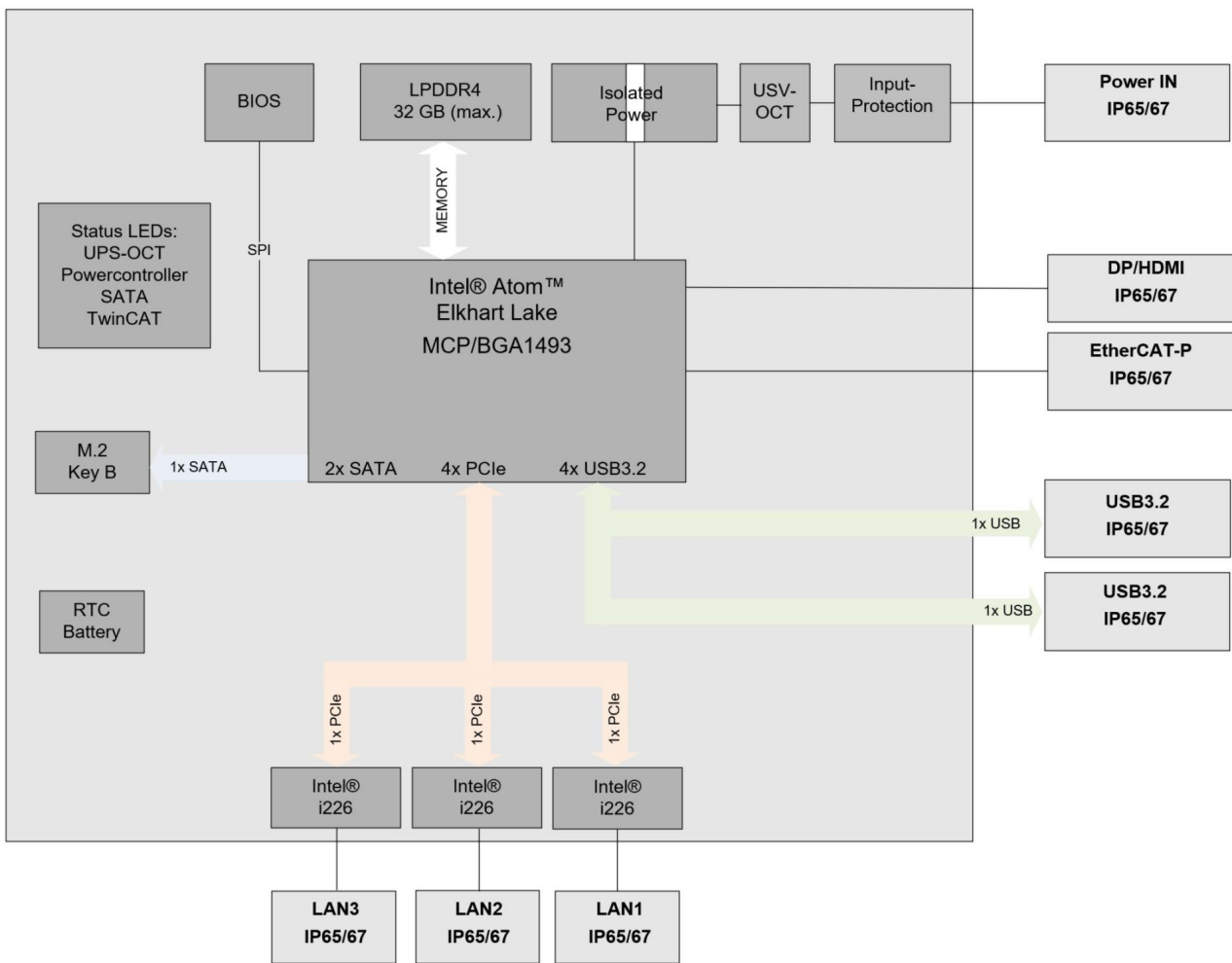


Fig. 1: CB8283 block diagram

5.2 List of features

● Availability of the processors



The list of features lists all the processors that can be ordered. Their actual availability depends on the manufacturer.

List of features	
CB8283	
CPU	Intel® Atom™ x6212RE (DC/1.5M/1.2GHz/TDP6W) Intel® Atom™ X6414RE (QC/1.5M/1.5GHZ/TDP9W) Intel® Atom™ X6425RE (QC/1.5M/1.9GHz/TDP12W)
Socket	Elkhart Lake, BGA1493, Multi-Chip Package (MCP)
Memory	OnBoard SDRAM-1.1V / LPDDR4, Dual channel (depending on CPU up to 3200 MT/s, max. 32 GB)
I/O front panel	1x EtherCAT P connection, IP65/67 1x power, IP65/67 1x DisplayPort (connection of an HDMI adapter for one HDMI signal possible), IP65/67 3x LAN 10/100/1000/2500, IP65/67 2x USB 3.2, IP65/67
I/O internal	1x M.2 (B) socket, signals dependent on chipset (see M.2 2242/2280k Key B (P1000) [► 21])
Graphic resolution	HDMI 1.4b: 3840x2160 @ 30 Hz DisplayPort 1.2a/eDP 1.3: 4096x2160 @ 60 Hz MIPI-DSI: 2560x1600 @ 60 Hz
RTC	CR2032 battery
BIOS	AMI® Aptio V
Power supply	20 V - 30 V input voltage overvoltage and undervoltage protection reverse polarity protection, UPS-OCT possible, electrically isolated
Format	135 x 75 mm

5.3 Specifications and documents

The following documents, specifications or webpages were used for the preparation of this manual or as further technical documentation respectively.

- **PCI specification**
 - Version 2.3 or 3.0
 - www.pcisig.com
- **PCI Express® Base Specification**
 - Version 5.0
 - www.pcisig.com
- **ACPI specification**
 - Version 5.0
 - www.acpi.info
- **ATA/ATAPI specification**
 - Version 7 Rev. 1
 - www.t13.org
- **USB specifications**
 - www.usb.org
- **SMBus specification**
 - Version 2.0
 - www.smbus.org
- **Intel® chip descriptions**
 - Intel® Core™ Processor Product Family datasheet
 - www.intel.com
- **Intel® chip description**
 - i226 Datasheet
 - www.intel.com
- **SMSC® chip description**
 - SCH3114 Datasheet (NDA required)
 - www.smsc.com
- **American Megatrends®**
 - Aptio™ Text Setup Environment (TSE) User Manual
 - www.ami.com
- **American Megatrends®**
 - Aptio™ 5.x Status Codes
 - www.ami.com

6 Detailed description

6.1 Power supply

The power supply conforms to IP65/67. The board is supplied with an isolated input voltage of nominally 24 V, which in reality may lie between 20 V and 30 V. In normal operation the DC/DC power rail is supplied with this voltage.

A UPS can also be implemented via an UOS-OCT signal (OCT = One Cable Technology).



UPS-OCT

The UPS OCT can only be implemented with the Beckhoff CU81XX-xxxx UPS.

6.2 CPU

The processors are multi-chip packages from Intel®. These MCPs are based on processors from the x6000E series (Elkhart Lake Gen11). Advanced energy-saving LPDDR4 technology enables memory extension of up to 32 GB, depending on the product variant.

Intel® processors of the x6000E series (Elkhart Lake Gen11) have an extended ambient temperature range and are therefore particularly suitable for use in industrial systems.

6.3 Memory

Four SDRAM memory modules up to a maximum of 32 GB are permanently installed on the CB8283 board.

Depending on the component variant, these are 4 GB or 8 GB DDR4 or LPDDR4 memory variants. Depending on the CPU used, a maximum clock frequency of 3200 MHz is supported.

6.4 M.2 socket

M.2 cards can easily and simply be inserted by plugging them into the slot and fixing them with a screw. Cards of different types have different recesses (keys). Depending on which types are supported, ports can accept expansion cards of one or more types. The M.2 socket of the CB8283 supports M.2 modules with Key B. SATA signals that allow an SSD to be connected are output via the interface.

7 Interfaces

7.1 Note on the use of cables

● **Requirement for the cabling!**



The cables used must meet certain requirements for most interfaces. For example, twisted and shielded cables are necessary for a reliable USB 2.0 connection. Limitations in the maximum cable length are also no rarity. All of these interface-specific requirements can be found in the respective specifications and must be observed accordingly.

NOTICE

IP65/67 cable type

The cables used must comply with IP65/67!

7.2 Interface overview

The interfaces of the CB8283 board are summarized in the figure below. The table below shows the function of the respective interface, as well as the manual page where you can find further information on this connection.

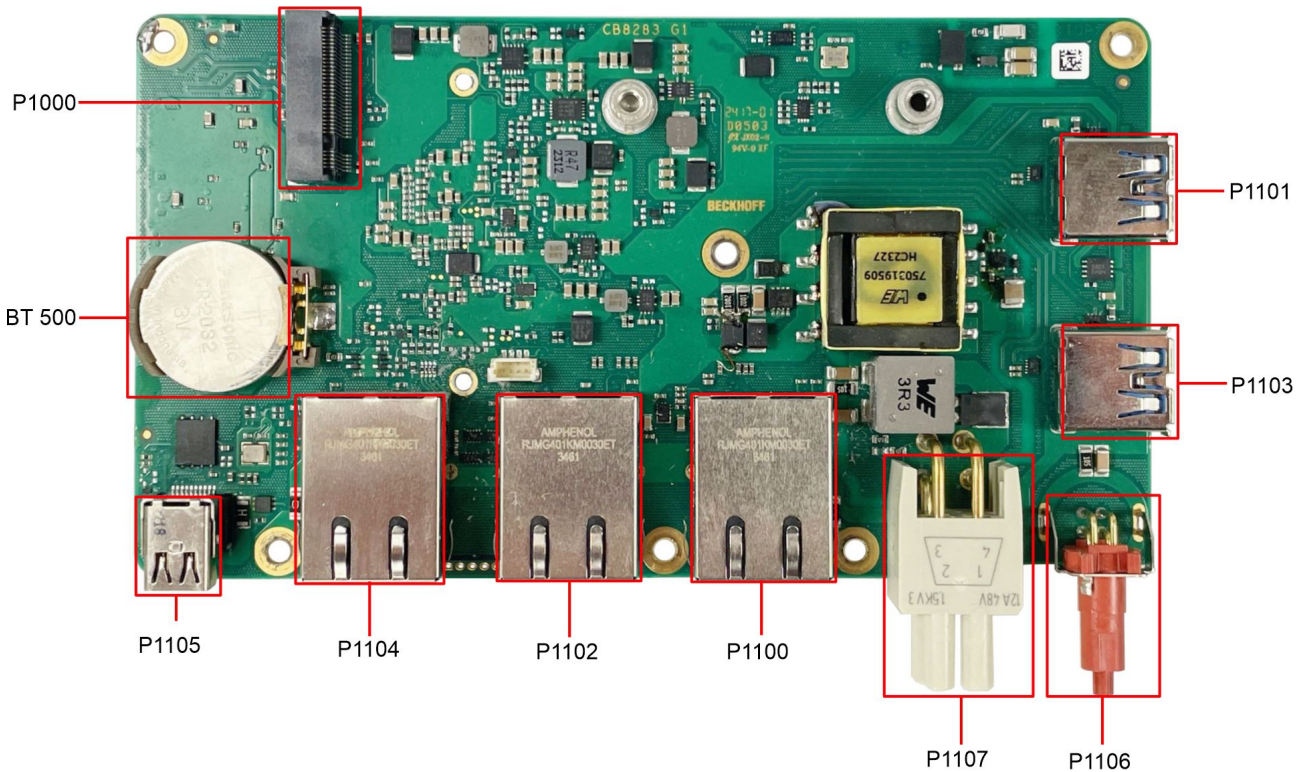


Fig. 2: CB8283 interface overview



Interface designation

The designation of the interfaces corresponds to the designation in the circuit diagram.

7.3 List of interfaces

Number	Function (designation)	Page
P1101	USB 3.2	USB 3.2 IP65/67 (P1103, P1101) [▶ 16]
P1103	USB 3.2	USB 3.2 IP65/67 (P1103, P1101) [▶ 16]
P1106	EtherCAT P	EtherCAT P IP65/67 (P1106) [▶ 17]
P1107	Vin / S UPS	Power connection IP65/67 (P1107) [▶ 18]
P1100	LAN 1	LAN IP65/67 (P1100, P1102, P1104) [▶ 19]
P1102	LAN 2	LAN IP65/67 (P1100, P1102, P1104) [▶ 19]
P1104	LAN 3	LAN IP65/67 (P1100, P1102, P1104) [▶ 19]
P1105	DP	Mini DisplayPort IP65/67 (P1105) [▶ 20]
BT500	Battery holder	Battery (BT500) [▶ 23]
P1000	M.2 socket Key B	M.2 2242/2280k Key B (P1000) [▶ 21]



Sequence of the interfaces

The list is in clockwise order, starting with the interface P1101 (USB3.2).

7.4 External interfaces

7.4.1 USB 3.2 IP65/67 (P1103, P1101)

USB channels 1 and 2 are each made available via a USB connector (P1103, P1101) in accordance with IP65/67.

The USB channels support the USB specification 3.2. Low-power and high-power modes are also specified. The maximum currents here are limited to 150 mA and 900 mA. Devices with their own current supply must be used for higher power demands. The USB interfaces are electronically protected.

All necessary settings for USB can be made in the BIOS. This applies to both USB interfaces. Note that the "USB Mouse and Keyboard" functionality of the BIOS setup is only required if the operating system does not provide USB support. Do not select this function for settings in the setup and for booting Windows with a connected USB mouse and keyboard, because this would result in significant performance limitations.



Fig. 3: P1103 and P1101-USB

Pin assignment USB3.2 connector		
Pin	Signal	Description
1	VCC	Supply voltage 5 V
2	D-	Data - (USB 2.0)
3	D+	Data + (USB 2.0)
4	GND	Ground
5	SSRX-	Receive line - (USB 3.2)
6	SSRX+	Receive line + (USB 3.2)
7	GND	Ground
8	SSTX-	Transmit line - (USB 3.2)
9	SSTX+	Transmit line + (USB 3.2)

7.4.2 EtherCAT P IP65/67 (P1106)

EtherCAT P (EtherCAT + Power) is an extension of the EtherCAT technology in the area of cabling. This IP65/67 connector allows you to use the four-core Ethernet cable (IP65/67) for data and for two electrically isolated, individually switchable 24 V/3 A power supplies. This allows you to cascade several EtherCAT devices. You only need one cable for the connection and power supply of I/O and field devices.

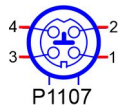


Fig. 4: P1106 EtherCAT P connection

Pin assignment EtherCAT P connection IP65/67		
Pin	Signal	Description
1	LAN41+	LAN signal + and ground
2	LAN40 +	LAN signal + and ground
3	LAN40 -	LAN signal - and supply voltage 24 V
4	LAN41 -	LAN signal - and supply voltage 24 V

7.4.3 Power connection IP65/67 (P1107)

The connection for the power supply is implemented as a 2x2-pin housing plug in accordance with IP65/67. The main power supply (24 V) for the module is on pin 2.

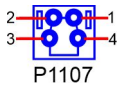


Fig. 5: P1107 Power connection

Pin assignment of the power plug:					
Description	Signal	Pin		Signal	Description
Supply voltage 24V	Vin	2	1	GND	Ground
PC Start: Input for starting and shutting down the PC. Low (0 V or open contact): PC starts. High (>3V): PC shuts down.	PC_START	3	4	PC_ACTIVE	PC status: Output of the PC status. The voltage corresponds to the positive supply voltage and can be loaded with 1A. Low (0 V): PC is off. High (Vin): PC is on.

● Function restrictions PC_Start switch

i Please note that there are system states in which the activation of a connected PC_Start switch is ignored by the system, e.g. during booting of a Windows operating system. In this case, repeat the operation of the switch after a few seconds. The same applies to connected PC_Start push buttons.

7.4.4 LAN IP65/67 (P1100, P1102, P1104)

The board has three 2.5 Gbit LAN connections in accordance with IP65/67. 10/100/1000/2500BaseT-compatible network components can be connected to all of them. The required speed is selected automatically. TSN, Auto-Cross and Auto-Negotiate are available as well as PXE and RPL functionality. Controller is Intel®'s i226-IT.

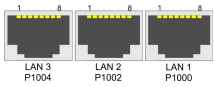


Fig. 6: P1000 P1002 P1004 LAN 2.5 IP65

Pin assignment of LAN connector		
Pin	Name	Description
1	LAN-0	LAN line 0 +
2	LAN-0#	LAN line 0 -
3	LAN-1	LAN line 1 +
4	LAN-2	LAN line 2 +
5	LAN-2#	LAN line 2 -
6	LAN-1	LAN line 1 -
7	LAN-3	LAN line 3 +
8	LAN-3#	LAN line 3 -

7.4.5 Mini DisplayPort IP65/67 (P1005)

The board has a Mini DisplayPort in accordance with IP65/67.

The interface additionally provides HDMI/DVI signals that can be used with aid of an adapter. Please consult your distributor with regard to a suitable adapter.

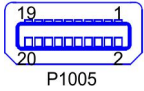


Fig. 7: P1005 Display Port IP65

Pin assignment Mini DisplayPort					
Description	Signal	Pin		Signal	Description
Ground	GND	1	2	HPD	Hot Plug Detect
Display Port Lane 0 +	L0	3	4	DP / HDMI	HDMI#
Display Port Lane 0 -	L#0	5	6	GND	Ground
Ground	GND	7	8	GND	Ground
Display Port Lane 1 +	L1	9	10	L3	Display Port Lane 3 +
Display Port Lane 1 -	L#1	11	12	L#3	Display Port Lane 3 -
Ground	GND	13	14	GND	Ground
Display Port Lane 2 +	L2	15	16	AUX	Auxiliary plus
Display Port Lane 2 -	L#2	17	18	AUX#	Auxiliary minus
Ground	GND	19	20	3.3 V	Supply voltage 3.3 V

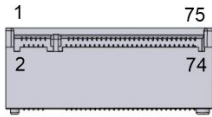
i Switching to HDMI

DisplayPort signals are led out via the interface by default. With the use of a level shifter cable the board switches the DisplayPort specification 1.1 automatically to HDMI signals.

7.5 Internal interfaces

7.5.1 M.2 2242/2280k Key B (P1000)

The CB8283 is equipped with an M.2 socket, into which an M.2-2242/2280 card (Key B) can be inserted. SATA signals (up to 3 Gb/s), which enable the connection of an M.2-SSD card, are fed out via this socket.



P1000

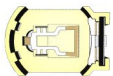
Fig. 8: P1000 M.2KeyB

Pin assignment M.2 2242/2280 connector					
Description	Signal	Pin		Signal	Description
Configuration pin	CFG3	1	2	3.3 V1	Standby supply voltage S3.3 V
Ground	GND1	3	4	3.3 V2	Standby supply voltage S3.3 V
Ground	GND2	5	6	FCPWROFF#	Full Card Power OFF active low
USB Channel 2 Data +	USB_D+	7	8	WDISABLE#	(not led out)
USB Channel 2 Data -	USB_D-	9	10	GPIO9 DAS DDS LED1	(not led out)
Ground	GND3	11	12	Connector Key	
Connector Key		13	14		
		15	16		
		17	18		
		19	20	GPIO5	(not led out)
Configuration pin	CFG 0	21	22	GPIO6	(not led out)
(not led out)	GPIO11	23	24	GPIO7	(not led out)
(not led out)	DPR	25	26	GPIO10	(not led out)
Ground	GND4	27	28	GPIO8	(not led out)
(not led out)	PER1# USB3 SSRX# SSICRX#	29	30	UIM_RST	(not led out)
(not led out)	PER1 USB3 SSRX SSICRX	31	32	UIM_CLK	(not led out)
Ground	GND5	33	34	UIM_DATA	(not led out)
(not led out)	PET1# USB3TX# SSICTX#	35	36	UIM_PWR	(not led out)
(not led out)	PET1 USB3TX SSICTX	37	38	DEVSLP	(not led out)
Ground	GND6	39	40	GPIO0	(not led out)
SATA Lane 1 Receive plus	PER0 SATAB	41	42	GPIO1	(not led out)
SATA Lane 1 Receive minus	PER0# SATAB#	43	44	GPIO2	(not led out)
Ground	GND7	45	46	GPIO3	(not led out)
SATA Lane 1 Transmit minus	PET0# SATAA#	47	48	GPIO4	(not led out)
SATA Lane 1 Transmit plus	PET0 SATAA	49	50	PRST#	PCIe Reset active low
Ground	GND8	51	52	CLKREQ#	(not led out)
(not led out)	REFCLK#	53	54	PEWAKE#	(not led out)
(not led out)	REFCLK	55	56	NC1	(not led out)
Ground	GND9	57	58	NC2	(not led out)
(not led out)	ANTCTL0	59	60	COEX3	(not led out)
(not led out)	ANTCTL1	61	62	COEX2	(not led out)
(not led out)	ANTCTL2	63	64	COEX1	(not led out)

Pin assignment M.2 2242/2280 connector					
Description	Signal	Pin		Signal	Description
(not led out)	ANTCTL3	65	66	SIM_DETECT	(not led out)
Powergood	RESET#	67	68	SUSCLK	Suspendclock
Configuration pin	CFG1	69	70	3.3V3	Standby supply voltage S3.3 V
Ground	GND10	71	72	3.3V4	Standby supply voltage S3.3 V
Ground	GND11	73	74	3.3V5	Standby supply voltage S3.3 V
Configuration pin	CFG2	75			

7.5.2 Battery (BT500)

The board is delivered with a CR2032 battery holder together with a 3 V battery.



BT 500

Fig. 9: BT500 battery

i UL conformity

All technical measures for UL conformity are already integrated on the board.

Accordingly, no additional actions are necessary for the connection of an RTC battery. The battery must be connected directly.

8 BIOS

8.1 Using the setup

Within the individual setup pages the last saved settings can be restored can at any time with F2 ("Previous Values"). Use F3 ("Optimized Defaults") to load the factory defaults. Use F2/F3 to load the complete set of settings and F4 to save them ("Save & Reset").

A "▶" sign in front of the menu item indicates that a submenu is available. Use the arrow keys to navigate between menu items. Use the Enter key to select menu items and call submenus or selection dialogs.

For each setup option a help text is displayed at the top right, which in many cases contains useful information about the option and permitted values, etc.

8.2 Main CB8283

Aptio Setup - AMI

Main Advanced Chipset Security Boot Save & Exit

<pre> Board Information Board CB8283 Revision 0 Bios Version 0.07 BIOSAPI Version 2.44.0002 Compute Die Information Name ElkhartLake Type Intel Atom(R) x6225RE Processor @ 1.90 GHz Speed 1900 MHz ID 0x90661 Stepping B0 Number of Processors 4Cores(s) / 4Thread(s) Microcode Revision 17 GT Info GT4 (0x4571) IGFX GOP Version 18.0.1044 Memory RC Version 0.0.4.111 Total Memory 8192 MB Memory Data Rate 3200 MTPS PCH Information Name EHL PCH Stepping B1 ME FW Version 15.40.30.2979 System Date [Sun 01/21/2024] System Time [09:57:31] </pre>	<pre> ↑: Select Screen ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit </pre>
--	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Board	None
Revision	None
Bios Version	None
BIOSAPI Version	None
Compute Die Information	None
Name	None
Type	None
Speed	None
ID	None
Stepping	None
Number of Processors	None
Microcode Revision	None
GT Info	None
IGFX GOP Version	None
Memory RC version	None
Total Memory	None
Memory Data Rate	None
PCH Information	None
Name	None
Stepping	None
ME FW Version	None
Memory Information	
System Date	Set the system date here.
System Time	Set the system time here.

8.3 Advanced

Aptio Setup - AMI

Main **Advanced** Chipset Security Boot Save & Exit

Power-Supply Type [ATX] SoftOff on Overheat [Disabled] Show postcode on screen [Disabled] ▶ RC ACPI Settings ▶ CPU Configuration ▶ Trusted Computing ▶ ACPI Settings ▶ Hardware Monitor ▶ Acoustic Management Configuration ▶ PCI Subsystem Settings ▶ USB Configuration ▶ Network Stack Configuration ▶ Power Controller Options ▶ NVMe Configuration ▶ RAM Disk Configuration ▶ Intel(R) Ethernet Controller I226-IT -00:A0:C9:00:00:00 ▶ Intel(R) Ethernet Controller I226-IT -00:A0:C9:00:00:00 ▶ Intel(R) Ethernet Controller I226-IT -00:A0:C9:00:00:00 ▶ User Password Management ▶ Driver Health	Select the Type of the Power Supply: AT/ATX ←: Select Screen ↓↑: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Power-Supply Type	ATX / AT
SoftOff on Overheat	Disabled / Enabled
Show postcode on screen	Disabled / Enabled
▶ RC ACPI Settings	Submenu: RC ACPI settings [▶ 27]
▶ CPU Configuration	Submenu: CPU Configuration [▶ 28]
▶ Trusted Computing	Submenu: Trusted Computing [▶ 30]
▶ ACPI Settings	Submenu: ACPI Settings [▶ 31]
▶ Hardware Monitor	Submenu: Hardware Monitor [▶ 31]
▶ Acoustic Management Configuration	Submenu: Acoustic Management Configuration [▶ 32]
▶ PCI Subsystem Settings	Submenu: PCI Subsystem Settings [▶ 33]
▶ USB Configuration	Submenu: USB Configuration [▶ 34]
▶ Network Stack Configuration	Submenu: Network Stack Configuration Disabled [▶ 35]
▶ Power Controller Options	Submenu: Power Controller Options [▶ 36]
▶ NVME Configuration	Submenu: NVMe Configuration [▶ 37]
▶ RAM Disk Configuration	Submenu: RAM Disk Configuration [▶ 37]
▶ Intel® Ethernet Controller I226-IT - 00:A0:C9:00:00:00	Submenu: Intel Ethernet Controller I226-IT [▶ 39]
▶ Intel® Ethernet Controller I226-IT - 00:A0:C9:00:00:00	Submenu: Intel Ethernet Controller I226-IT [▶ 40]
▶ Intel® Ethernet Controller I226-IT - 00:A0:C9:00:00:00	Submenu: Intel Ethernet Controller I226-IT [▶ 41]
▶ User Password Management	Submenu: User Password Management [▶ 42]
▶ Driver Health	Submenu: Driver Health [▶ 42]

8.3.1 RC ACPI settings

Aptio Setup - AMI

Advanced

<p>RC ACPI Settings</p> <p>PTID Support [Enabled]</p> <p>PECI Access Method [Direct I/O]</p> <p>Native PCIE Enable [Enabled]</p> <p>Native ASPM [Auto]</p> <p>BDAT ACPI Table Support [Disabled]</p> <p>ACPI Debug [Disabled]</p> <p>MSI enabled [Enabled]</p>	<p>PTID Support will be loaded if enabled.</p> <p>←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
---	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
RC ACPI Settings	
PTID Support	Enabled / Disabled
PECI Access Method	Direct I/O / ACPI
Native PCIE Enable	Enabled / Disabled
Native ASPM	Auto / Enabled / Disabled
BDAT ACPI Table Support	Disabled / Enabled
ACPI Debug	Disabled / Enabled
MSI enabled	Enabled / Disabled

8.3.2 CPU Configuration

Aptio Setup - AMI
Advanced

<p>CPU Configuration</p> <pre> Intel ATom(R) x6212RE Processor @ 1.20GHz ID 0x90661 Speed 1200 MHz L1 Data Cache 32 KB x 2 L1 Instruction Cache 32 KB x 2 L2 Cache 1536 KB x 2 L3 Cache 4 MB L4 Cache N/A VMX Supported SMX/TXT Not Supported CPU Flex Ratio Override [Disabled] CPU Flex Ratio Settings 12 Hardware Prefetcher [Enabled] Intel (VMX) Virtualization Technology [Enabled] PECI [Enabled] Active Processor Cores [All] BIST [Disabled] AP threads Idle Manner [MWAIT Loop] AES [Enabled] MachineCheck [Enabled] MonitorMWait [Enabled] ▶ CPU SMM Enhancement #AC Split Lock [Disabled] </pre>	<p>▲ Enable/Disable CPU Flex Ratio Programming</p> <hr/> <p>←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p> <p style="text-align: center;">▼</p>
---	---

Version 2.22.1282 Copyright (C) 2023 AMI

BIOS entry	Options
CPU Configuration	
Type	None
ID	None
Speed	None
L1 Data Cache	None
L1 Instruction Cache	None
L2 Cache	None
L3 Cache	None
L4 Cache	None
VMX	None
SMX/TXT	None
CPU Flex Ratio Override	Disabled / Enabled
CPU Flex Ratio Settings	None
Hardware Prefetcher	Enabled / Disabled
Adjacent Cache Line Prefetch	Enabled / Disabled
Intel (VMX) Virtualization Technology	Enabled / Disabled
PECI	Enabled / Disabled
Active Processor Cores	All / 1 / 2 / 3
BIST	Disabled / Enabled
AP threads Idle Manner	MWait Loop / Halt Loop / Run Loop
AES	Enabled / Disabled
MachineCheck	Enabled / Disabled
Monitor MWait	Enabled / Disabled
▶ CPU SMM Enhancement	Submenu: CPU SMM Enhancement [▶ 29]
#AC Split Lock	Disabled / Enabled

8.3.2.1 CPU SMM Enhancement

Aptio Setup - AMI
Advanced

CPU SMM enhancement SMM Use Delay Indication [Enabled] SMM Use Block Indication [Enabled] SMM Use SMM en-US Indication [Enabled]	Enable/Disable usage of SMM_DELAYED MSR for MP sync in SMI ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	--

Version 2.22.1282 Copyright (C) 2023 AMI

BIOS entry	Options
CPU SMM Enhancement Information	
SMM Use Delay Indication	Enabled / Disabled
SMM Use Block Indication	Enabled / Disabled
SMM Use SMM en - US Indication	Enabled / Disabled

8.3.3 Trusted Computing

Aptio Setup - AMI
Advanced

<pre> TPM 2.0 Device Found Firmware Version: 600.15 Vendor: INTC Security Device Support [Enable] Active PCR banks SHA256 Available PCR banks SHA256, SHA384, SM3 SHA256 PCR Bank [Enabled] SHA384 PCR Bank [Disabled] SM3_256 PCR Bank [Disabled] Pending operation [None] Platform Hierarchy [Enabled] Storage Hierarchy [Enabled] Endorsement Hierarchy [Enabled] Physical Presence Spec Version [1.3] TPM 2.0 InterfaceType [CRB] Device Select [Auto] </pre>	<p>Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.</p> <hr/> <pre> ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit </pre>
--	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Configuration	
Security Device Support	Enable / Disable
SHA256 PCR Bank	Enabled / Disabled
SHA384 PCR Bank	Disabled / Enabled
SM_3256PCR Bank	Disabled/ Enabled
Pending Operation	None / TPM Clear
Platform Hierarchy	Enabled / Disabled
Storage Hierarchy	Enabled / Disabled
Endorsement Hierarchy	Enabled / Disabled
Physical Presence Spec Version	1.3 / 1.2
TPM 2.0 InterfaceType	None
Device Select	Auto / TPM 1.2 / TPM 2.0

8.3.4 ACPI Settings

Aptio Setup - AMI
Advanced

ACPI Settings Enable ACPI Auto Configuration [Disabled] Enable Hibernation [Enabled] Lock Legacy Resources [Disabled]	Enables or Disables BIOS ACPI Auto Configuration. ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
ACPI Settings	
Enable ACPI Auto Configuration	Disabled / Enabled
Enable Hibernation	Enabled / Disabled
Lock Legacy Resources	Disabled / Enabled

8.3.5 Hardware Monitor

Aptio Setup - AMI
Advanced

PC Health Status CPU dig. : +44 'C MB Temp : +33 'C 5V : +5.10 V	←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
PC Health Status	None

8.3.6 Acoustic Management Configuration

Aptio Setup - AMI
Advanced

Acoustic Management Configuration HDD not found	←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
--	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Acoustic Management Configuration	
HDD not found	None

8.3.7 PCI Subsystem Settings

Aptio Setup - AMI

Advanced

<p>AMI PCI Driver Version A5.01.22</p> <p>PCI Settings Common for all Devices: BME DMA Mitigation [Disabled]</p> <p>Change Settings of the Following PCI Devices:</p> <p>WARNING: Changing PCI Device(s) settings may have unwanted side effects! System may HANG! PROCEED WITH CAUTION.</p>	<p>Re-enable Bus Master Attribute disabled during Pci enumeration for PCI Bridges after SMM Locked</p>
<pre> →: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit </pre>	

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
AMI PCI Driver Version:	None
PCI Settings Common for all Devices:	
BME DMA Mitigation	Disabled / Enabled

8.3.8 USB Configuration

Aptio Setup - AMI	
Advanced	
USB Configuration	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
USB Module Version 25	
USB Controllers: 1 XHCI	
USB Devices: 1 Keyboard	
Legacy USB Support [Enabled]	
XHCI Hand-off [Enabled]	
USB Mass Storage Driver Support [Enabled]	
USB hardware delays and time-outs:	←: Select Screen
USB transfer time-out [20 sec]	↑↓: Select Item
Device reset time-out [20 sec]	Enter: Select
Device power-up delay [Auto]	+/-: Change Opt.
	F1: General Help
	F2: Previous Values
	F3: Optimized Defaults
	F4: Save & Reset
	ESC: Exit
Version 2.22.1282 Copyright (C) 2024 AMI	

BIOS entry	Options
USB Configuration	
USB Module Version	None
USB Devices	None
Legacy USB support	Enabled / Disabled / Auto
XHCI Hand-off	Enabled / Disabled
USB Mass Storage Driver Support	Enabled / Disabled
USB hardware delays and time-outs:	
USB transfer time-out	1 / 5 / 10 / 20 sec
Device reset time-out	10 / 20 / 30 / 40 sec
Device power-up delay	Auto / Manual

8.3.9 Network Stack Configuration Disabled

Aptio Setup - AMI
Advanced

Network Stack [Disabled]	Enable/Disable UEFI Network <hr/> ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
--------------------------	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Network Stack	Disabled / Enabled

8.3.10 Network Stack Configuration Enabled

Aptio Setup - AMI
Advanced

Network Stack [Enabled] Ipv4 PXE Support [Disabled] Ipv4 HTTP Support [Disabled] Ipv6 PXE Support [Disabled] Ipv6 HTTP Support [Disabled] PXE boot wait time 0 Media detect count 1	Enable/Disable UEFI Network <hr/> ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Network Stack	Enabled / Disabled
Ipv4 PXE Support	Enabled / Disabled
Ipv4 HTTP Support	Enabled / Disabled
Ipv6 PXE Support	Enabled / Disabled
Ipv6 HTTP Support	Enabled / Disabled
PXE boot wait time	None
Media detect count	None

8.3.11 Power Controller Options

Aptio Setup - AMI

Advanced

Bootloader Version 1.02-01 Firmware Version 1.02-69 Mainboard Serial No Mainboard Prod. Date (Week.Year) -1.-1 Mainboard BootCount 21 Mainboard Operation Time 154600min (257h) Voltage (Min/Max) 5.10V / 5.20V Temperature (Min/Max) 23'C /60'C Enable Us in onboard EtherCAT-P [Disabled] Enable Up in onboard EtherCAT-P [Disabled] WatchDogTimer Mode [Normal Mode] WDT OSBoot Timeout [Disabled]	Select Power line for external USB devices, if powered-down ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
--	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Bootloader version	None
Firmware version	None
Mainboard Serial No	None
Mainboard Prod. Date (Week.Year)	None
Mainboard BootCount	None
Mainboard Operation Time	None
Voltage (Min/Max)	None
Temperature (Min/Max)	None
Enable Us in onboard EtherCAT-P	Disabled / Enabled
Enable Up in onboard EtherCAT-P	Disabled / Enabled
WatchDogTimer Mode	Normal Mode / Compatibility Mode
WDT OSBoot Timeout	Disabled / 45/60/75...225/240/255 Seconds

8.3.12 NVMe Configuration

Aptio Setup - AMI
Advanced

NVMe controller and Drive information No NVME Device Found	→: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
NVMe Configuration	
No NVME Device Found	None

8.3.13 RAM Disk Configuration

Aptio Setup - AMI
Advanced

Disk Memory Type: [Boot Service Data] ▶ Create raw ▶ Create from file Created RAM disk list: Remove selected RAM disk(s).	Specifies type of memory to use from available memory pool in system to create a disk →: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Disk Memory Type:	Boot Service Data / Reserved
▶ Create raw	Submenu: <u>C</u> reate raw [▶ 38]
▶ Create from file	None
Created RAM disk list:	
Remove selected RAM disk(s).	None

8.3.13.1 Create raw

Aptio Setup - AMI
Advanced

Size (Hex): 1 Create & Exit Discard & Exit	The valid RAM disk size should be multiples of the RAM disk block size. ←: Select Screen ↓↑: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Size (Hex):	None
Create & Exit	None
Discard & Exit	None

8.3.14 Intel Ethernet Controller I226-IT

Aptio Setup - AMI
Advanced

UEFI Driver Device Name PCI Device ID Link Status MAC Address	Intel (R) Pro/1000 Open Source 4.9.99 PCI-E Intel (R) Ethernet Controller I226-IT 125D [Disconnected] 00:A0:C9:00:00:00	←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	--	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
UEFI Driver	None
Device Name	None
PCI Device ID	None
Link Status	None
MAC Address	None

8.3.15 Intel Ethernet Controller I226-IT

Aptio Setup - AMI
Advanced

UEFI Driver Device Name PCI Device ID Link Status MAC Address	Intel (R) Pro/1000 Open Source 4.9.99 PCI-E Intel (R) Ethernet Controller I226-IT 125D [Disconnected] 00:A0:0C9:00:00:00	←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	---	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
UEFI Driver	None
Device Name	None
PCI Device ID	None
Link Status	None
MAC Address	None

8.3.16 Intel Ethernet Controller I226-IT

Aptio Setup - AMI
Advanced

UEFI Driver Device Name PCI Device ID Link Status MAC Address	Intel (R) Pro/1000 Open Source 4.9.99 PCI-E Intel (R) Ethernet Controller I226-IT 125D [Disconnected] 00:A0:C9:00:00:00	←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	--	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
UEFI Driver	None
Device Name	None
PCI Device ID	None
Link Status	None
MAC Address	None

8.3.17 User Password Management

Aptio Setup - AMI
Advanced

Admin Password Status Change Admin Password	Not Installed	Input old admin password if it was set, then you can change the password to a new one. After the change action, you may need input the new password when you enter UI. The new password must be between 8 and 32 chars include lowercase, uppercase alphabetic, number, and symbol. Input an empty
		←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Admin Password Status	None
Change Admin Password	None

8.3.18 Driver Health

Aptio Setup - AMI
Advanced

<ul style="list-style-type: none"> ▶ Intel(R) PRO/1000 Open Source 8.3.10 PCI-E Healthy ▶ Intel(R) PRO/1000 Open Source 4.9.99 PCI-E Healthy 	Provides Health Status for the Drivers/Controllers	
		←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
▶ Intel(R) PRO/1000 Open Source 8.3.10 PCI-E	None
▶ Intel(R) PRO/1000 Open Source 4.9.99 PCI-E	None

8.4 Chipset

Aptio Setup - AMI

Main Advanced **Chipset** Security Boot Save & Exit

<ul style="list-style-type: none"> ▶ System Agent (SA) Configuration ▶ PCH-IO Configuration 	<p style="text-align: center;">System Agent (SA) Parameters</p> <p>←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
---	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
▶ System Agent (SA) Configuration	Submenu: System Agent (SA) Configuration [▶ 43]
▶ PCH-IO Configuration	Submenu: PCH-IO Configuration [▶ 48]

8.4.1 System Agent (SA) Configuration

Aptio Setup - AMI

Chipset

<p>System Agent (SA) Configuration</p> <p>VT-d Supported</p> <ul style="list-style-type: none"> ▶ Graphics Configuration <p>VT-d [Enabled] X2APIC Opt Out [Enmabled] DMA Control Guarantee [Disabled] IGD VTD Enable [Enabled] IOP VTD Enable [Enabled] GNA Device (B0:D8:F0) [Enabled] CRID Support [Disabled] Above 4GB MMIO BIOS assignment [Enabled]</p>	<p style="text-align: center;">Graphics Configuration</p> <p>←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
--	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
System Agent (SA) Configuration	
VT-d	None
▶ Graphics Configuration	Submenu: Graphics Configuration [▶ 44]
VT-d	Enabled / Disabled
X2APIC Opt Out	Disabled / Enabled
DMA Control Guarantee	Disabled / Enabled
IGD VTD Enable	Enabled / Disabled
IOP VTD Enable	Enabled / Disabled
GNA Device (B0:D8:F0)	Enabled / Disabled
CRID Support	Disabled / Enabled
Above 4GB MMIO BIOS assignment	Enabled / Disabled

8.4.1.1 Graphics Configuration

```

Aptio Setup - AMI
Chipset

Graphics Configuration
Graphics Turbo IMON Current      31
Skip Scanning of External Gfx Card [Disabled]

Primary Display [Auto]
▶ External Gfx Card Primary Display Configuration
Internal Graphics [Auto]
Headlessmode [Disabled]
GTT Size [8MB]
Aperture Size [128MB]
PSMI SUPPORT [Disabled]
DVMT Pre-Allocated [60M]
DVMT Total Gfx Mem [256M]
DiSM Size [0GB]
Intel Graphics Pei Display Peim [Disabled]
VDD Enable [Enabled]
Configure GT for use [Enabled]
PAVP Enable [Enabled]
Cdynmax Clamping Enable [Disabled]
Cd Clock Frequency [Max CDClock freq based on Reference Clk]

VBT Select [eDP]
▶ LCD Control
▶ Intel (R) Ultrabook Event Support

Graphics turbo IMON current values supported (14-31)

←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Reset
ESC: Exit

Version 2.22.1282 Copyright (C) 2024 AMI
    
```

BIOS entry	Options
Graphics Configuration	
Graphics Turbo IMON Current	None
Skip Scanning of External Gfx Card	Disabled / Enabled
Primary Display	Auto / IGFX / PEG Slot / PCH PCI / HG
▶ External Gfx Card Primary Display Configuration	Submenu: External Gfx Card Primary Display Configuration [▶ 45]
Internal Graphics	Auto / Disabled / Enabled
GTT Size	2 / 4 / 8 MB
Aperture Size	128 / 256 / 512 / 1024 MB
PSMI SUPPORT	Disabled / Enabled
DVMT Pre-Allocated	0M, 32M...64M, 96M, 128M, 160M
DVMT Total Gfx Mem	128M / 256M / MAX
DiSM Size	0 – 7 GB
Intel Graphics Pei Display Peim	Disabled / Enabled
VDD Enable	Enabled / Disabled
Configure GT for use	Disabled / Enabled
PAVP Enable	Enabled / Disabled
Cdynmax Clamping Enable	Disabled / Enabled
Cd Clock Frequency	172.8 / 307.2 / 556.8 / 652.8 Mhz Max CdClock freq based on Reference Clk
VBT Select	eDP / MIPI
▶ LCD Control	Submenu: LCD Control [▶ 46]
▶ Intel® Ultrabook Event Support	Submenu: Intel Ultrabook Event Support [▶ 47]

8.4.1.1.1 External Gfx Card Primary Display Configuration

Aptio Setup - AMI
Chipset

External Gfx Card Primary Display Configuration Primary PCIE [Auto]	Select Auto/PCIE1/PCIE2/PCIE3/PCIE4/PCIE5/PCIE6/PCIE7 of D28:F0/F1/F2/F3/F4/F5/F6/F7, PCIE8/PCIE9/PCIE10/PCIE11/PCIE12/PCIE13/PCIE14/PCIE15 of D29:F0/F1/F2/F3/F4/F5/F6/F7, PCIE16/PCIE17/PCIE18/PCIE19 of D27:F0/F1/F2/F3, Graphics device should be Primary PCIE.
←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit	

Version 2.22.1282 Copyright (C) 2023 AMI

BIOS entry	Options
External Gfx Card Primary Display Configuration	
Primary PCIE	Auto / PCI1 - PCIE19

8.4.1.1.2 LCD Control

Aptio Setup - AMI
Chipset

<p>LCD Control</p> <p>Primary IGFX Boot Display [VBIOS Default] LCD Panel Type [VBIOS DEFAULT] Panel Scaling [Auto] Backlight Control [PWM Normal] Active LFP [eDP Port-A] Panel Color Depth [18 Bit] Backlight Brightness 255</p>	<p>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</p> <hr/> <p>→: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
--	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
LCD Control	
Primary IGFX Boot Display	VBIOS Default / EFP / LFP / EFP3 / EFP2 / EFP3
LCD Panel Type	VBIOS Default / Various LVDS Resolutions
Panel Scaling	Auto / Off / Force Scaling
Backlight Control	PWM Normal / PWM Inverted
Active LFP	eDP Port / No eDP
Panel Color Depth	18 Bit / 24 Bit
Backlight Brightness	None

8.4.1.1.3 Intel Ultrabook Event Support

Aptio Setup - AMI
Chipset

Intel (R) Ultrabook Event Support IUER Slate Enable [Disabled] IUER Dock Enable [Disabled]	Enable/Disable IUER Slate Functionality ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
--	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Intel® Ultrabook Event Support	
IUER Slate Enable	Disabled / Enabled
IUER Dock Enable	Disabled / Enabled

8.4.2 PCH-IO Configuration

Aptio Setup - AMI
Chipset

<p>PCH-IO Configuration</p> <ul style="list-style-type: none"> ▶ PCI Express Configuration ▶ SATA Configuration ▶ USB Configuration ▶ HD Audio Configuration <p>State After G3 [S0 State]</p> <p>Compatible Revision ID [Disabled]</p> <p>Legacy IO Low Latency [Enabled]</p> <p>Enable TCO Timer [Disabled]</p>	<p>PCI Express Configuration settings</p> <hr/> <p>←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
--	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
PCH-IO Configuration	
▶ PCI Express Configuration	Submenu: PCI Express Configuration [▶ 49]
▶ SATA Configuration	Submenu: SATA Configuration [▶ 64]
▶ USB Configuration	Submenu: USB Configuration [▶ 67]
▶ HD Audio Configuration	Submenu: HD Audio Configuration [▶ 68]
State After G3	S0 State / S5 State
Compatible Revision ID	None
Legacy IO Low Latency	Disabled / Enabled
Enable TCO Timer	Enabled / Disabled

8.4.2.1 PCI Express Configuration

Aptio Setup - AMI
Chipset

PCI Express Configuration DMI Link ASPM Control [Disabled] PCIE Port assigned to LAN Disabled Peer Memory Write Enable [Disabled] Compliance Test Mode [Disabled] PCH PCI Express Clock Gating [Disabled] PCI Express Root Port 1 Lane configured as USB/SATA/UFS PCI Express Root Port 2 Lane configured as USB/SATA/UFS ▶ PCI Express Root Port 3 ▶ PCI Express Root Port 4 ▶ PCI Express Root Port 5 PCI Express Root Port 6 Lane configured as USB/SATA/UFS ▶ PCI Express Root Port 7	The control of Active State Power Management of the DMI Link. ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
PCI Express Configuration	
DMI Link ASPM Control	Disabled / L0s / L1 / L0sL1 / Auto
PCIE Port assigned to LAN	Disabled
Peer Memory Write Enable	Disabled / Enabled
Compliance Test Mode	Disabled / Enabled
PCH PCI Express Clock Gating	Disabled / Enabled
PCI Express Root Port 1	None
PCI Express Root Port 2	None
▶ PCI Express Root Port 3	Submenu: PCI Express Root Port 3 [▶ 50]
▶ PCI Express Root Port 4	Submenu: PCI Express Root Port 4 [▶ 53]
▶ PCI Express Root Port 5	Submenu: PCI Express Root Port 5 [▶ 56]
PCI Express Root Port 6	None
▶ PCI Express Root Port 7	Submenu: PCI Express Root Port 7 [▶ 60]

8.4.2.1.1 PCI Express Root Port 3

Aptio Setup - AMI
Chipset

PCI Express Root Port 3 [Enabled]	▲ Control the PCI Express Root Port.
Connection Type [Slot]	⇐: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
ASPM [Disabled]	
L1 Substates [Disabled]	
ACS [Enabled]	
PTM [Disabled]	
DPC [Enabled]	
EDPC [Enabled]	
URR [Disabled]	
FER [Disabled]	
NFER [Disabled]	
CER [Disabled]	
SEFE [Disabled]	
SENFE [Disabled]	
SECE [Disabled]	
PME SCI [Enabled]	
Hot Plug [Disabled]	
Advanced Error Reporting [Enabled]	
PCIe Speed [Auto]	
Transmitter Half Swing [Disabled]	
Detect Timeout 0	
Extra Bus Reserved 0	
Reserved Memory 10	
Reserved I/O 4	
PCH PCIe LTR Congguration	
LTR [Enabled]	
Snoop Latency Override [Auto]	
Non Snoop Latency Override [Auto]	
Force LTR Override [Disabled]	
LTR Lock [Disabled]	
▶ Extra Options	▼

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
PCI Express Root Port 5	Enabled / Disabled
Connection Type	Slot / Built-in
ASPM	Disabled / Enabled
L1 Substates	Disabled / L1.1 & L1.2 / L1.1
ACS	Enabled / Disabled
PTM	Enabled / Disabled
DPC	Enabled / Disabled
EDPC	Enabled / Disabled
URR	Disabled / Enabled
FER	Disabled / Enabled
NFER	Disabled / Enabled
CER	Disabled / Enabled
SEFE	Disabled / Enabled
SENF	Disabled / Enabled
SECE	Disabled / Enabled
PME SCI	Disabled / Enabled
Hot Plug	Enabled / Disabled
Advanced Error Reporting	Enabled / Disabled
PCIe Speed	Auto / Gen1 / Gen2 / Gen3
Transmitter Half Swing	Disabled / Enabled
Detect Timeout	None
Extra Bus Reserved	None
Reserved Memory	None
Reserved I/O	None
PCH PCIe LTR Configuration	
LTR	Enabled / Disabled
Snoop Latency Override	Auto / Manual / Disabled
Non Snoop Latency Override	Auto / Manual / Disabled
Force LTR Override	Disabled / Enabled
LTR Lock	Disabled / Enabled
▶ Extra Options	Submenu: Extra Options [▶ 52]

8.4.2.1.1.1 Extra Options

Aptio Setup - AMI
Chipset

Detect Non-Compliance Device [Disabled] Prefetchable Memory 10 Reserved Memory Alignment 1 Prefetchable Memory Alignment 1	Detect Non-Compliance Device PCI Express Device. If enable, it will take more time at Post time.
←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit	

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Detect Non-Compliance Device	Disabled / Enabled
Prefetchable Memory	None
Reserved Memory Alignment	None
Prefetchable Memory Alignment	None

8.4.2.1.2 PCI Express Root Port 4

Aptio Setup - AMI
Chipset

PCI Express Root Port 4 [Enabled]	▲ Control the PCI Express Root Port.
Connection Type [Slot]	⇐: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
ASPM [Disabled]	
L1 Substates [Disabled]	
ACS [Enabled]	
PTM [Disabled]	
DPC [Enabled]	
EDPC [Enabled]	
URR [Disabled]	
FER [Disabled]	
NFER [Disabled]	
CER [Disabled]	
SEFE [Disabled]	
SENFE [Disabled]	
SECE [Disabled]	
PME SCI [Enabled]	
Hot Plug [Disabled]	
Advanced Error Reporting [Enabled]	
PCIe Speed [Auto]	
Transmitter Half Swing [Disabled]	
Detect Timeout 0	
Extra Bus Reserved 0	
Reserved Memory 10	
Reserved I/O 4	
PCH PCIe LTR Congguration	
LTR [Enabled]	
Snoop Latency Override [Auto]	
Non Snoop Latency Override [Auto]	
Force LTR Override [Disabled]	
LTR Lock [Disabled]	
▶ Extra Options	▼

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
PCI Express Root Port 5	Enabled / Disabled
Connection Type	Slot / Built-in
ASPM	Disabled / Enabled
L1 Substates	Disabled / L1.1 & L1.2 / L1.1
ACS	Enabled / Disabled
PTM	Enabled / Disabled
DPC	Enabled / Disabled
EDPC	Enabled / Disabled
URR	Disabled / Enabled
FER	Disabled / Enabled
NFER	Disabled / Enabled
CER	Disabled / Enabled
SEFE	Disabled / Enabled
SENF	Disabled / Enabled
SECE	Disabled / Enabled
PME SCI	Disabled / Enabled
Hot Plug	Enabled / Disabled
Advanced Error Reporting	Enabled / Disabled
PCIe Speed	Auto / Gen1 / Gen2 / Gen3
Transmitter Half Swing	Disabled / Enabled
Detect Timeout	None
Extra Bus Reserved	None
Reserved Memory	None
Reserved I/O	None
PCH PCIe LTR Configuration	
LTR	Enabled / Disabled
Snoop Latency Override	Auto / Manual / Disabled
Non Snoop Latency Override	Auto / Manual / Disabled
Force LTR Override	Disabled / Enabled
LTR Lock	
LTR Lock	Disabled / Enabled
► Extra Options	Submenu: Extra Options [► 55]

8.4.2.1.2.1 Extra Options

Aptio Setup - AMI
Chipset

Detect Non-Compliance Device [Disabled] Prefetchable Memory 10 Reserved Memory Alignment 1 Prefetchable Memory Alignment 1	Detect Non-Compliance Device PCI Express Device. If enable, it will take more time at Post time.
←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit	

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Detect Non-Compliance Device	Disabled / Enabled
Prefetchable Memory	None
Reserved Memory Alignment	None
Prefetchable Memory Alignment	None

8.4.2.1.3 PCI Express Root Port 5

Aptio Setup - AMI
Chipset

PCI Express Root Port 5 [Enabled]	▲ Control the PCI Express Root Port.
Connection Type [Slot]	▲ Control the PCI Express Root Port. ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
ASPM [Disabled]	
L1 Substates [Disabled]	
ACS [Enabled]	
Multi-VC [Enabled]	
▶ VC to TC Mapping	
PTM [Disabled]	
DPC [Enabled]	
EDPC [Enabled]	
URR [Disabled]	
FER [Disabled]	
NFER [Disabled]	
CER [Disabled]	
SEFE [Disabled]	
SENF [Disabled]	
SECE [Disabled]	
PME SCI [Enabled]	
Hot Plug [Disabled]	
Advanced Error Reporting [Enabled]	
PCIe Speed [Auto]	
Transmitter Half Swing [Disabled]	
Detect Timeout 0	
Extra Bus Reserved 0	
Reserved Memory 10	
Reserved I/O 4	
PCH PCIe LTR Congguration	
LTR [Enabled]	
Snoop Latency Override [Auto]	
Non Snoop Latency Override [Auto]	
Force LTR Override [Disabled]	
LTR Lock [Disabled]	
▶ Extra Options	

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
PCI Express Root Port 5	Enabled / Disabled
Connection Type	Slot / Built-in
ASPM	Disabled / Enabled
L1 Substates	Disabled / L1.1 & L1.2 / L1.1
ACS	Enabled / Disabled
Multi-VC	Enabled / Disabled
▶ VC to TC Mapping	Submenu: VC to TC Mapping [▶ 58]
PTM	Enabled / Disabled
DPC	Enabled / Disabled
EDPC	Enabled / Disabled
URR	Disabled / Enabled
FER	Disabled / Enabled
NFER	Disabled / Enabled
CER	Disabled / Enabled
SEFE	Disabled / Enabled
SENF	Disabled / Enabled
SECE	Disabled / Enabled
PME SCI	Disabled / Enabled
Hot Plug	Enabled / Disabled
Advanced Error Reporting	Enabled / Disabled
PCIe Speed	Auto / Gen1 / Gen2 / Gen3
Transmitter Half Swing	Disabled / Enabled
Detect Timeout	None
Extra Bus Reserved	None
Reserved Memory	None
Reserved I/O	None
PCH PCIe LTR Configuration	
LTR	Enabled / Disabled
Snoop Latency Override	Auto / Manual / Disabled
Non Snoop Latency Override	Auto / Manual / Disabled
Force LTR Override	Disabled / Enabled
LTR Lock	
LTR Lock	Disabled / Enabled
▶ Extra Options	
Submenu: Extra Options [▶ 59]	

8.4.2.1.3.1 VC to TC Mapping

Aptio Setup - AMI
Chipset

TC0 TC1 TC2 TC3 TC4 TC5 TC6 TC7	VC0 [VC0] [VC0] [VC0] [VC0] [VC0] [VC1] [VC1]	Maps PCIe traffic class 1 to a virtual channel. ←: Select Screen ↓↑: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
--	--	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
TC0	None
TC1	VC0 / VC1
TC2	VC0 / VC1
TC3	VC0 / VC1
TC4	VC0 / VC1
TC5	VC0 / VC1
TC6	VC1 / VC0
TC7	VC1 / VC0

8.4.2.1.3.2 Extra Options

Aptio Setup - AMI
Chipset

Detect Non-Compliance Device [Disabled] Prefetchable Memory 10 Reserved Memory Alignment 1 Prefetchable Memory Alignment 1	Detect Non-Compliance Device PCI Express Device. If enable, it will take more time at Post time.	←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	--	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Detect Non-Compliance Device	Disabled / Enabled
Prefetchable Memory	None
Reserved Memory Alignment	None
Prefetchable Memory Alignment	None

8.4.2.1.4 PCI Express Root Port 7

Aptio Setup - AMI
Chipset

PCI Express Root Port 7 [Enabled]	▲ Control the PCI Express Root Port.
Connection Type [Slot]	▲ Control the PCI Express Root Port. ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
ASPM [Disabled]	
L1 Substates [Disabled]	
ACS [Enabled]	
Multi-VC [Enabled]	
▶ VC to TC Mapping	
PTM [Disabled]	
DPC [Enabled]	
EDPC [Enabled]	
URR [Disabled]	
FER [Disabled]	
NFER [Disabled]	
CER [Disabled]	
SEFE [Disabled]	
SENF [Disabled]	
SECE [Disabled]	
PME SCI [Enabled]	
Hot Plug [Disabled]	
Advanced Error Reporting [Enabled]	
PCIe Speed [Auto]	
Transmitter Half Swing [Disabled]	
Detect Timeout 0	
Extra Bus Reserved 0	
Reserved Memory 10	
Reserved I/O 4	
PCH PCIe LTR Congguration	
LTR [Enabled]	
Snoop Latency Override [Auto]	
Non Snoop Latency Override [Auto]	
Force LTR Override [Disabled]	
LTR Lock [Disabled]	
▶ Extra Options	

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
PCI Express Root Port 7	Enabled / Disabled
Connection Type	Slot / Built-in
ASPM	Disabled / Enabled
L1 Substates	Disabled / L1.1 & L1.2 / L1.1
ACS	Enabled / Disabled
Multi-VC	Enabled / Disabled
▶ VC to TC Mapping	Submenu: VC to TC Mapping [▶ 62]
PTM	Enabled / Disabled
DPC	Enabled / Disabled
EDPC	Enabled / Disabled
URR	Disabled / Enabled
FER	Disabled / Enabled
NFER	Disabled / Enabled
CER	Disabled / Enabled
SEFE	Disabled / Enabled
SENF	Disabled / Enabled
SECE	Disabled / Enabled
PME SCI	Disabled / Enabled
Hot Plug	Enabled / Disabled
Advanced Error Reporting	Enabled / Disabled
PCIe Speed	Auto / Gen1 / Gen2 / Gen3
Transmitter Half Swing	Disabled / Enabled
Detect Timeout	None
Extra Bus Reserved	None
Reserved Memory	None
Reserved I/O	None
PCH PCIe LTR Configuration	
LTR	Enabled / Disabled
Snoop Latency Override	Auto / Manual / Disabled
Non Snoop Latency Override	Auto / Manual / Disabled
Force LTR Override	Disabled / Enabled
LTR Lock	
LTR Lock	Disabled / Enabled
▶ Extra Options	
Submenu: Extra Options [▶ 63]	

8.4.2.1.4.1 VC to TC Mapping

Aptio Setup - AMI
Chipset

TC0 TC1 TC2 TC3 TC4 TC5 TC6 TC7	VC0 [VC0] [VC0] [VC0] [VC0] [VC0] [VC1] [VC1]	Maps PCIe traffic class 1 to a virtual channel. ←: Select Screen ↓↑: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
--	--	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
TC0	None
TC1	VC0 / VC1
TC2	VC0 / VC1
TC3	VC0 / VC1
TC4	VC0 / VC1
TC5	VC0 / VC1
TC6	VC1 / VC0
TC7	VC1 / VC0

8.4.2.1.4.2 Extra Options

Aptio Setup - AMI
Chipset

Detect Non-Compliance Device [Disabled] Prefetchable Memory 10 Reserved Memory Alignment 1 Prefetchable Memory Alignment 1	Detect Non-Compliance Device PCI Express Device. If enable, it will take more time at Post time.	←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	--	--

Version 2.22.1282 Copyright (C) 2025 AMI

BIOS entry	Options
Detect Non-Compliance Device	Disabled / Enabled
Prefetchable Memory	None
Reserved Memory Alignment	None
Prefetchable Memory Alignment	None

8.4.2.2 SATA Configuration

Aptio Setup - AMI
Chipset

<p>SATA Configuration</p> <p>SATA Controller(s) [Enabled]</p> <p>SATA Ports Multipler Mode [Disabled]</p> <p>SATA Test Mode [Disabled]</p> <p>▶ Software Feature Mask Configuration</p> <p>Aggressive LPM Support [Enabled]</p> <p>Serial ATA Port 0 Empty</p> <p>Software Preserve Unknown</p> <p>Port 0 [Enabled]</p> <p>Hot Plug [Disabled]</p> <p>Configured As eSATA Hot Plug Supported</p> <p>External [Disabled]</p> <p>Spin Up Device [Disabled]</p> <p>SATA Device Type [Hard Disk Drive]</p> <p>Topology [Unknown]</p> <p>SATA Port 0 DevSlp [Disabled]</p> <p>SATA Port 0 RxPolarity [Disabled]</p> <p>DITO Configuration [Disabled]</p> <p>Serial ATA Port 1 Empty</p> <p>Software Preserve Unknown</p> <p>Port 1 [Enabled]</p> <p>Hot Plug [Disabled]</p> <p>Configured As eSATA Hot Plug Supported</p> <p>External [Disabled]</p> <p>Spin Up Device [Disabled]</p> <p>SATA Device Type [Hard Disk Drive]</p> <p>Topology [Unknown]</p> <p>SATA Port 1 DevSlp [Enabled]</p> <p>SATA Port 1 RxPolarity [Disabled]</p> <p>DITO Configuration [Disabled]</p> <p>Serial ATA Port 2 Empty</p> <p>Software Preserve Unknown</p> <p>Port 2 [Enabled]</p> <p>Hot Plug [Disabled]</p> <p>Configured As eSATA Hot Plug Supported</p> <p>External [Disabled]</p> <p>Spin Up Device [Disabled]</p> <p>SATA Device Type [Hard Disk Drive]</p> <p>Topology [Unknown]</p> <p>SATA Port 2 DevSlp [Disabled]</p> <p>SATA Port 2 RxPolarity [Disabled]</p> <p>DITO Configuration [Disabled]</p>	<p>▲ Enable/Disable SATA Device.</p> <hr/> <p>←: Select Screen</p> <p>↑↓: Select Item</p> <p>Enter: Select</p> <p>+/-: Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Reset</p> <p>ESC: Exit</p>
--	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
SATA Configuration	
SATA Controller(s)	Enabled / Disabled
SATA Mode Selection	None
SATA Test Mode	Disabled / Enabled
► Software Feature Mask Configuration	Submenu: Software Feature Mask Configuration [► 66]
Aggressive LPM Support	Enabled / Disabled
Serial ATA Port 0	None
Software Preserve	None
Port 0	Enabled / Disabled
Hot Plug	Disabled / Enabled
Configured As eSATA	None
External	Disabled / Enabled
Spin Up Device	Disabled / Enabled
SATA Device Type	Hard Disk Drive / Solid State Drive
Topology	Unknown / ISATA / Direct Connect / Flex / M2
SATA Port 0 DevSlp	Enabled / Disabled
SATA Port 0 RxPolarity	Enabled / Disabled
DITO Configuration	Disabled / Enabled
Serial ATA Port 1	None
Software Preserve	None
Port 1	Enabled / Disabled
Hot Plug	Disabled / Enabled
Configured As eSATA	None
External	Disabled / Enabled
Spin Up Device	Disabled / Enabled
SATA Device Type	Hard Disk Drive / Solid State Drive
Topology	Unknown / ISATA / Direct Connect / Flex / M2
SATA Port 1 DevSlp	Enabled / Disabled
DITO Configuration	Disabled / Enabled
Serial ATA Port 2	None
Software Preserve	None
Port 2	Enabled / Disabled
Hot Plug	Disabled / Enabled
Configured As eSATA	None
External	Disabled / Enabled
Spin Up Device	Disabled / Enabled
SATA Device Type	Hard Disk Drive / Solid State Drive
Topology	Unknown / ISATA / Direct Connect / Flex / M2
SATA Port 2 DevSlp	Enabled / Disabled
DITO Configuration	Disabled / Enabled

8.4.2.2.1 Software Feature Mask Configuration

Aptio Setup - AMI
Chipset

Software Feature Mask Configuration HDD Unlock [Enabled] LED Locate [Enabled]	If enabled, indicates that the HDD password unlock in the OS is enabled. →: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Software Feature Mask Configuration	
HDD Unlock	Enabled / Disabled
LED Locate	Enabled / Disabled

8.4.2.3 USB Configuration

Aptio Setup - AMI
Chipset

USB Configuration USB\$ Link Speed Selection [GEN2] USB Port Disable Override [Disabled] USB Device/HOST Mode Override [Disabled] USB USCI ACPI device [Disabled]	This option is to select USB3 Link Speed GEN1 or GEN2 →: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
USB Configuration	
USB3 Link Speed Selection	Gen2 / Gen1
USB Port Disable Override	Disabled / Select Per-Pin
USB Device/HOST Mode Override	Disabled / Select Per-Pin
USB USCI ACPI device	Disabled / Enabled

8.4.2.4 HD Audio Configuration

Aptio Setup - AMI
Chipset

HD Audio Subsystem Configuration Settings HD Audio [Enabled] Audio DSP [Enabled] Audio DSP Compliance Mode [Non-UAA (IntelSST)] Audio Link Mode [HA Audio Link] HDA-Link Codec Select [Platform Onboard] ▶ HD Audio Advanced Configuration ▶ HD Audio DSP Features Configuration	Control Detection of the HD-Audio device. Disabled = HDA will be unconditionally disabled Enabled = HDA will be unconditionally enabled.
←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit	

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
HD Audio Subsystem Configuration Settings	
HD Audio	Enabled / Disabled
Audio DSP	Enabled / Disabled
Audio DSP Compliance Mode	Non-UAA (IntelSST) / UAA (HDA Inbox/IntelSST)
Audio Link Mode	SSP (I2S) / HD Audio Link / SoundWire / Advanced Link Config
HDA-Link Codec Select	Platform Onboard / External Kit
▶ HD Audio Advanced Configuration	Submenu: HD Audio Advanced Configuration ▶ 69
▶ HD Audio DSP Features Configuration	Submenu: HD Audio Subsystem Features Configuration (ACPI) ▶ 70

8.4.2.4.1 HD Audio Advanced Configuration

Aptio Setup - AMI
Chipset

HD Audio Subsystem Advanced Configuration Settings		
iDisplay Audio Disconnect	[Disabled]	▲ Disconnects SDI2 signal to hide/disable iDisplay Audio Codec.
Codec Sx Wake Capability	[Disabled]	
PME Enable	[Disabled]	
Statically Switchable BCLK Clock Frequency Configuration		
HD Audio Link Frequency	[24 MHz]	▲ ▼ ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
iDisplay Audio Link Frequency	[96 MHz]	
iDisplay Audio Link T-Mode	[8T Mode]	
Autonomous Clock Stop SNDW #1	[Disabled]	
Autonomous Clock Stop SNDW #2	[Disabled]	
Autonomous Clock Stop SNDW #3	[Disabled]	
Autonomous Clock Stop SNDW #4	[Disabled]	
Data On Active Interval Select SNDW #1	[4 clock periods]	
Data On Active Interval Select SNDW #2	[4 clock periods]	
Data On Active Interval Select SNDW #3	[4 clock periods]	
Data On Active Interval Select SNDW #4	[4 clock periods]	
Data On Delay Select SNDW #1	[3 clock periods]	
Data On Delay Select SNDW #2	[3 clock periods]	
Data On Delay Select SNDW #3	[3 clock periods]	
Data On Delay Select SNDW #4	[3 clock periods]	

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
HD Audio Subsystem Advanced Configuration Settings	
iDisplay Audio Disconnect	Disabled / Enabled
Codec Sx Wake Capability	Disabled / Enabled
PME Enable	Disabled / Enabled
Statically Switchable BCLK Clock DPC Frequency Configuration:	
HD Audio Link Frequency	6 MHz / 12 MHz / 24 MHz
iDisplay Audio Link Frequency	48 MHz / 96 MHz
iDisplay Audio Link T-Mode FER	2T Mode / 4T Mode / 8T Mode / 16T Mode
Autonomous Clock Stop SNDW #1	Disabled / Enabled
Autonomous Clock Stop SNDW #2	Disabled / Enabled
Autonomous Clock Stop SNDW #3	Disabled / Enabled
Autonomous Clock Stop SNDW #4	Disabled / Enabled
Data On Active Interval Select SNDW #1	3 / 4 / 5 / 6 clock periods
Data On Active Interval Select SNDW #2	3 / 4 / 5 / 6 clock periods
Data On Active Interval Select SNDW #3	3 / 4 / 5 / 6 clock periods
Data On Active Interval Select SNDW #4	3 / 4 / 5 / 6 clock periods
Data On Delay Select SNDW #1	2 / 3 clock periods
Data On Delay Select SNDW #2	2 / 3 clock periods
Data On Delay Select SNDW #3	2 / 3 clock periods
Data On Delay Select SNDW #4	2 / 3 clock periods

8.4.2.4.2 HD Audio Subsystem Features Configuration (ACPI)

Aptio Setup - AMI
Chipset

<p>HD Audio Subsystem Features Configuration (ACPI)</p> <p>Audio DSP NHLT Endpoints Configuration:</p> <p>NHLT External Table [Disabled] DMIC [4 Mic Array] Bluetooth [Enabled] I2S [Enabled] I2S Codec Select [Realtek ALC5660I]</p> <p>Audio DSP Feature Support:</p> <p>WoV (Wake on Voice) [Enabled] Bluetooth Sideband [Disabled] BT Intel HFP [Disabled] BT Intel A2DP [Disabled] Codec based VAD [Disabled] DSP based Speech [Disabled] Pre-Processingbg Disabled Voice Activity Detection [Windows 10 Voice Activation]</p> <p>Audio DSP Pre/Post-Processing Module Support:</p> <p>Waves Post-process [Disabled] DTS [Disabled] IntelSST Speech [Disabled] Dolby [Disabled] Waves Pre-process [Disabled] Audyssey [Disabled] Maxim Smart AMP [Disabled] ForteMedia SAMSoft [Disabled] Sound Research IP [Disabled] Conexant Pre-Process [Disabled] Conexant Smart Amp [Disabled] Realtek Post-Process [Disabled] Realtek Smart Amp [Disabled] Icepower IP MFX sub module [Disabled] Icepower IP EFX sub module [Disabled] Icepower IP SFX sub module [Disabled] Voice Preprocessing [Disabled] Custom Module 'Alpha' [Disabled] Custom Module 'Beta' [Disabled] Custom Module 'Gamma' [Disabled]</p>	<p>▲ Load external NHLT table from binary file instead of using NHLT built from policy setting.</p> <hr/> <p>←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
---	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
HD Audio Subsystem Features Configuration (ACPI)	
Audio DSP NHLT Endpoints Configuration:	
NHLT External Table	Disabled / Enabled
DMIC	Disabled / 1 / 2 / 4 Mic Array
Bluetooth	Enabled / Disabled
I2S	Enabled / Disabled
I2S Codec Select	Realtek ALC274 / Realtek ALC5660I / Disabled
Audio DSP Feature Support:	
WoV (Wake on Voice)	Enabled Disabled
Bluetooth Sideband	Disabled / Enabled
BT Intel HFP	None
BT Intel A2DP	None
Codec based VAD	Disabled / Enabled
DSP based Speech	None
Pre-Processing disabled	
Voice Activity Detection	Intel Wake on Voice / Windows 10 Voice Activation
Audio DSP Pre/Post-Processing Module Support:	
Waves Post-process	Disabled / Enabled
DTS	Disabled / Enabled
IntelSST Speech	Disabled / Enabled
Dolby	Disabled / Enabled
Waves Pre-process	Disabled / Enabled
Audyssey	Disabled / Enabled
Maxim Smart AMP	Disabled / Enabled
ForteMedia SAMSoft	Disabled / Enabled
Sound Research IP	Disabled / Enabled
Conexant Pre-Process	Disabled / Enabled
Conexant Smart Amp	Disabled / Enabled
Realtek Post-Process	Disabled / Enabled
Realtek Smart Amp	Disabled / Enabled
Icepower IP MFX sub module	Disabled / Enabled
Icepower IP EFX sub module	Disabled / Enabled
Icepower IP SFX sub module	Disabled / Enabled
Voice Preprocessing	Disabled / Enabled
Custom Module 'Alpha'	Disabled / Enabled
Custom Module 'Beta'	Disabled / Enabled
Custom Module 'Gamma'	Disabled / Enabled

8.5 Security

Aptio Setup - AMI
Main Advanced Chipset **Security** Boot Save & Exit

Password Description Minimum length 3 Maximum length 20 Administrator Password User Mode available [Enabled]	Set Administrator Password ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	--

▶ Secure Boot

Version 2.22.1282. Copyright (C) 2024 AMI

BIOS entry	Options
Password Description	
Minimum Length	None
Maximum Length	None
Administrator Password	Set an administrator password here.
User Mode available	Enabled / Disabled
Secure Boot menu	Submenu: Secure Boot [▶ 73]

8.5.1 Secure Boot

Aptio Setup - AMI
Security

System Mode Secure Boot Secure Boot Mode ▶ Restore Factory Keys ▶ Reset To Setup Mode ▶ Key Management	User [Enabled] Active [Custom]	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key(PK) is enrolled and the System is in User mode. The mode change requires platform reset ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	---	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
System Mode	None
Secure Boot	Enabled / Disabled
Secure Boot Mode	Standard / Custom
▶ Restore Factory Keys	Press enter key
▶ Reset To Setup Mode	Press enter key
▶ Key Management	Submenu: <u>Key Management</u> [▶ <u>74</u>]

8.5.1.1 Key Management

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <ul style="list-style-type: none"> ▶ Restore Factory Keys ▶ Reset To Setup Mode ▶ Export Secure Boot variables ▶ Enroll Efi Image <p>Device Guard Ready</p> <ul style="list-style-type: none"> ▶ Remove 'UEFI CA' from DB ▶ Restore DB defaults <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th>Secure Boot variable</th> <th>Size</th> <th>Keys</th> <th>Key Source</th> </tr> </thead> <tbody> <tr> <td>▶ Platform Key(PK)</td> <td>862</td> <td>1</td> <td>Test (AMI)</td> </tr> <tr> <td>▶ Key Exchange Keys</td> <td>1560</td> <td>1</td> <td>Factory</td> </tr> <tr> <td>▶ Authorized Signatures</td> <td>3143</td> <td>2</td> <td>Factory</td> </tr> <tr> <td>▶ Forbidden Signatures</td> <td>10588</td> <td>220</td> <td>Factory</td> </tr> <tr> <td>▶ Authorized TimeStamps</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> <tr> <td>▶ OsRecovery Signatures</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> </tbody> </table>	Secure Boot variable	Size	Keys	Key Source	▶ Platform Key(PK)	862	1	Test (AMI)	▶ Key Exchange Keys	1560	1	Factory	▶ Authorized Signatures	3143	2	Factory	▶ Forbidden Signatures	10588	220	Factory	▶ Authorized TimeStamps	0	0	No Keys	▶ OsRecovery Signatures	0	0	No Keys	<p>Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode</p> <hr/> <p>←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
Secure Boot variable	Size	Keys	Key Source																										
▶ Platform Key(PK)	862	1	Test (AMI)																										
▶ Key Exchange Keys	1560	1	Factory																										
▶ Authorized Signatures	3143	2	Factory																										
▶ Forbidden Signatures	10588	220	Factory																										
▶ Authorized TimeStamps	0	0	No Keys																										
▶ OsRecovery Signatures	0	0	No Keys																										

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
Factory Key Provision	Disabled / Enabled
▶ Restore Factory Keys	Press enter key
▶ Reset To Setup Mode	Press enter key
▶ Export Secure Boot variables	Press enter key
▶ Enroll Efi Image	Press enter key
Device Guard Ready	
▶ Remove 'UEFI CA' from DB	Press enter key
▶ Restore DB defaults	Press enter key
Secure Boot variables	
▶ Platform Key(PK)	Press enter key
▶ Key Exchange Keys	Press enter key
▶ Authorized Signatures	Press enter key
▶ Forbidden Signatures	Press enter key
▶ Authorized TimeStamps	Press enter key
▶ OS Recovery Signatures	Press enter key

8.5.1.1.1 Restore factory keys

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Secure Boot variable</td> <td style="width: 10%;">Siz</td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> </tr> <tr> <td>> Platform Key (PK)</td> <td>86</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td>156</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Authorized Signatures</td> <td>314</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Forbidden Signatures</td> <td>10588</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Authorized TimeStamps</td> <td>0</td> <td>0</td> <td>No Keys</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> OsRecovery Signatures</td> <td>0</td> <td>0</td> <td>No Keys</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Secure Boot variable	Siz							> Platform Key (PK)	86							> Key Exchange Keys	156							> Authorized Signatures	314							> Forbidden Signatures	10588							> Authorized TimeStamps	0	0	No Keys					> OsRecovery Signatures	0	0	No Keys					<p>Force System to User Mode. Install factory default Secure Boot key databases</p>
Secure Boot variable	Siz																																																								
> Platform Key (PK)	86																																																								
> Key Exchange Keys	156																																																								
> Authorized Signatures	314																																																								
> Forbidden Signatures	10588																																																								
> Authorized TimeStamps	0	0	No Keys																																																						
> OsRecovery Signatures	0	0	No Keys																																																						

Install factory defaults

Press 'Yes' to proceed 'No' to cancel

Yes	No
-----	----

	<p>elect Screen</p> <p>elect Item</p> <p>: Select</p> <p>Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Reset</p> <p>ESC: Exit</p>
--	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
▶ Restore Factory Keys	see box

8.5.1.1.2 Reset To Setup Mode

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Secure Boot variable</td> <td style="width: 10%;">Siz</td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> </tr> <tr> <td>> Platform Key (PK)</td> <td>86</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td>156</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Authorized Signatures</td> <td>314</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Forbidden Signatures</td> <td>10588</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Authorized TimeStamps</td> <td>0</td> <td>0</td> <td>No Keys</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> OsRecovery Signatures</td> <td>0</td> <td>0</td> <td>No Keys</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Secure Boot variable	Siz							> Platform Key (PK)	86							> Key Exchange Keys	156							> Authorized Signatures	314							> Forbidden Signatures	10588							> Authorized TimeStamps	0	0	No Keys					> OsRecovery Signatures	0	0	No Keys					<p>Delete all Secure Boot key databases from NVRAM</p>
Secure Boot variable	Siz																																																								
> Platform Key (PK)	86																																																								
> Key Exchange Keys	156																																																								
> Authorized Signatures	314																																																								
> Forbidden Signatures	10588																																																								
> Authorized TimeStamps	0	0	No Keys																																																						
> OsRecovery Signatures	0	0	No Keys																																																						

Reset To Setup Mode

Deleting all variables will reset the System to Setup Mode
Do you want to proceed?

Yes	No
-----	----

	<p>elect Screen</p> <p>elect Item</p> <p>: Select</p> <p>Change Opt.</p> <p>eneral Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Reset</p> <p>ESC: Exit</p>
--	---

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
Restore To Setup Mode	see box

8.5.1.1.3 Export Secure Boot Variables

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Secure Boot variable</td> <td style="width: 10%;">Size</td> <td style="width: 10%;">K</td> <td style="width: 50%;"></td> </tr> <tr> <td>> Platform Key (PK)</td> <td>862</td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td>1560</td> <td></td> <td></td> </tr> <tr> <td>> Authorized Signatures</td> <td>3143</td> <td></td> <td></td> </tr> <tr> <td>> Forbidden Signatures</td> <td>10588</td> <td>22</td> <td></td> </tr> <tr> <td>> Authorized TimeStamps</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> <tr> <td>> OsRecovery Signatures</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> </table>	Secure Boot variable	Size	K		> Platform Key (PK)	862			> Key Exchange Keys	1560			> Authorized Signatures	3143			> Forbidden Signatures	10588	22		> Authorized TimeStamps	0	0	No Keys	> OsRecovery Signatures	0	0	No Keys	<p>Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device</p> <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="text-align: center;">File System</p> <p style="text-align: center;">No Valid File System Available</p> <p style="text-align: center;">Ok</p> </div> <p>: Select Screen : Select Item ter: Select -: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
Secure Boot variable	Size	K																											
> Platform Key (PK)	862																												
> Key Exchange Keys	1560																												
> Authorized Signatures	3143																												
> Forbidden Signatures	10588	22																											
> Authorized TimeStamps	0	0	No Keys																										
> OsRecovery Signatures	0	0	No Keys																										

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
Export Secure Boot Variables	File System, see box

8.5.1.1.4 Enroll Efi Image

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Secure Boot variable</td> <td style="width: 10%;">Size</td> <td style="width: 10%;">K</td> <td style="width: 50%;"></td> </tr> <tr> <td>> Platform Key (PK)</td> <td>862</td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td>1560</td> <td></td> <td></td> </tr> <tr> <td>> Authorized Signatures</td> <td>3143</td> <td></td> <td></td> </tr> <tr> <td>> Forbidden Signatures</td> <td>10588</td> <td>22</td> <td></td> </tr> <tr> <td>> Authorized TimeStamps</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> <tr> <td>> OsRecovery Signatures</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> </table>	Secure Boot variable	Size	K		> Platform Key (PK)	862			> Key Exchange Keys	1560			> Authorized Signatures	3143			> Forbidden Signatures	10588	22		> Authorized TimeStamps	0	0	No Keys	> OsRecovery Signatures	0	0	No Keys	<p>Allow the image to run in Secure Boot mode.</p> <p>Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db)</p> <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="text-align: center;">File System</p> <p style="text-align: center;">No Valid File System Available</p> <p style="text-align: center;">Ok</p> </div> <p>: Select Screen : Select Item ter: Select -: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
Secure Boot variable	Size	K																											
> Platform Key (PK)	862																												
> Key Exchange Keys	1560																												
> Authorized Signatures	3143																												
> Forbidden Signatures	10588	22																											
> Authorized TimeStamps	0	0	No Keys																										
> OsRecovery Signatures	0	0	No Keys																										

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
Enroll Efi Image	see box

8.5.1.1.5 Remove UEFI CA from DB

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Secure Boot variable</td> <td style="width: 10%;">Siz</td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> </tr> <tr> <td>> Platform Key (PK)</td> <td>86</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td>156</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Authorized Signatures</td> <td>314</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Forbidden Signatures</td> <td>10588</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Authorized TimeStamps</td> <td>0</td> <td>0</td> <td>No Keys</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> OsRecovery Signatures</td> <td>0</td> <td>0</td> <td>No Keys</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Secure Boot variable	Siz									> Platform Key (PK)	86									> Key Exchange Keys	156									> Authorized Signatures	314									> Forbidden Signatures	10588									> Authorized TimeStamps	0	0	No Keys							> OsRecovery Signatures	0	0	No Keys							<p>Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in Authorized Signature database (db)</p> <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="text-align: center;">Remove 'UEFI CA' from DB</p> <p style="text-align: center;">Press 'Yes' to proceed 'No' to cancel</p> <hr/> <p style="text-align: center;">Yes No</p> </div> <p>elect Screen</p> <p>elect Item</p> <p>: Select</p> <p>Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Reset</p> <p>ESC: Exit</p>
Secure Boot variable	Siz																																																																						
> Platform Key (PK)	86																																																																						
> Key Exchange Keys	156																																																																						
> Authorized Signatures	314																																																																						
> Forbidden Signatures	10588																																																																						
> Authorized TimeStamps	0	0	No Keys																																																																				
> OsRecovery Signatures	0	0	No Keys																																																																				

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
Remove 'UEFI CA' from DB	see box

8.5.1.1.6 Restore DB defaults

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Secure Boot variable</td> <td style="width: 10%;">Siz</td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> </tr> <tr> <td>> Platform Key (PK)</td> <td>86</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td>156</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Authorized Signatures</td> <td>314</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Forbidden Signatures</td> <td>10588</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> Authorized TimeStamps</td> <td>0</td> <td>0</td> <td>No Keys</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>> OsRecovery Signatures</td> <td>0</td> <td>0</td> <td>No Keys</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Secure Boot variable	Siz									> Platform Key (PK)	86									> Key Exchange Keys	156									> Authorized Signatures	314									> Forbidden Signatures	10588									> Authorized TimeStamps	0	0	No Keys							> OsRecovery Signatures	0	0	No Keys							<p>Restore DB variable to factory defaults</p> <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="text-align: center;">Restore DB defaults</p> <p style="text-align: center;">Press 'Yes' to proceed 'No' to cancel</p> <hr/> <p style="text-align: center;">Yes No</p> </div> <p>elect Screen</p> <p>elect Item</p> <p>: Select</p> <p>Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Reset</p> <p>ESC: Exit</p>
Secure Boot variable	Siz																																																																						
> Platform Key (PK)	86																																																																						
> Key Exchange Keys	156																																																																						
> Authorized Signatures	314																																																																						
> Forbidden Signatures	10588																																																																						
> Authorized TimeStamps	0	0	No Keys																																																																				
> OsRecovery Signatures	0	0	No Keys																																																																				

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
Restore DB Faults	see box

8.5.1.1.7 Platform Key (PK)

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr><th colspan="4" style="text-align: center;">Platform Key (PK)</th></tr> <tr><td colspan="4" style="text-align: center;">Details</td></tr> <tr><td colspan="4" style="text-align: center;">Export</td></tr> <tr><td colspan="4" style="text-align: center;">Update</td></tr> <tr><td colspan="4" style="text-align: center;">Delete</td></tr> </table> <table style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr> <th style="text-align: left;">Secure Boot variable</th> <th style="text-align: left;">Size</th> <th style="text-align: left;">Ke</th> <th style="text-align: left;">Ke</th> </tr> <tr> <td>> Platform Key (PK)</td> <td>862</td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td>1560</td> <td></td> <td></td> </tr> <tr> <td>> Authorized Signatures</td> <td>3143</td> <td>2</td> <td>Factory</td> </tr> <tr> <td>> Forbidden Signatures</td> <td>10588</td> <td>220</td> <td>Factory</td> </tr> <tr> <td>> Authorized TimeStamps</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> <tr> <td>> OsRecovery Signatures</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> </table>	Platform Key (PK)				Details				Export				Update				Delete				Secure Boot variable	Size	Ke	Ke	> Platform Key (PK)	862			> Key Exchange Keys	1560			> Authorized Signatures	3143	2	Factory	> Forbidden Signatures	10588	220	Factory	> Authorized TimeStamps	0	0	No Keys	> OsRecovery Signatures	0	0	No Keys	<p>Enroll Factory Defaults or load certificates from a file:</p> <ol style="list-style-type: none"> 1.Public Key Certificate: <ol style="list-style-type: none"> a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image (SHA256) <p>Key Source: Factory, External, Mixed</p> <hr/> <p>←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
Platform Key (PK)																																																	
Details																																																	
Export																																																	
Update																																																	
Delete																																																	
Secure Boot variable	Size	Ke	Ke																																														
> Platform Key (PK)	862																																																
> Key Exchange Keys	1560																																																
> Authorized Signatures	3143	2	Factory																																														
> Forbidden Signatures	10588	220	Factory																																														
> Authorized TimeStamps	0	0	No Keys																																														
> OsRecovery Signatures	0	0	No Keys																																														

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
Platform Key (PK)	see box

8.5.1.1.8 Key Exchange Keys

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr><th colspan="4" style="text-align: center;">Key Exchange Keys</th></tr> <tr><td colspan="4" style="text-align: center;">Details</td></tr> <tr><td colspan="4" style="text-align: center;">Export</td></tr> <tr><td colspan="4" style="text-align: center;">Update</td></tr> <tr><td colspan="4" style="text-align: center;">Append</td></tr> <tr><td colspan="4" style="text-align: center;">Delete</td></tr> </table> <table style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr> <th style="text-align: left;">Secure Boot variable</th> <th style="text-align: left;">Size</th> <th style="text-align: left;">Ke</th> <th style="text-align: left;">Ke</th> </tr> <tr> <td>> Platform Key (PK)</td> <td>862</td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td>1560</td> <td></td> <td></td> </tr> <tr> <td>> Authorized Signatures</td> <td>3143</td> <td></td> <td></td> </tr> <tr> <td>> Forbidden Signatures</td> <td>10588</td> <td>220</td> <td>Factory</td> </tr> <tr> <td>> Authorized TimeStamps</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> <tr> <td>> OsRecovery Signatures</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> </table>	Key Exchange Keys				Details				Export				Update				Append				Delete				Secure Boot variable	Size	Ke	Ke	> Platform Key (PK)	862			> Key Exchange Keys	1560			> Authorized Signatures	3143			> Forbidden Signatures	10588	220	Factory	> Authorized TimeStamps	0	0	No Keys	> OsRecovery Signatures	0	0	No Keys	<p>Enroll Factory Defaults or load certificates from a file:</p> <ol style="list-style-type: none"> 1.Public Key Certificate: <ol style="list-style-type: none"> a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image (SHA256) <p>Key Source: Factory, External, Mixed</p> <hr/> <p>←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
Key Exchange Keys																																																					
Details																																																					
Export																																																					
Update																																																					
Append																																																					
Delete																																																					
Secure Boot variable	Size	Ke	Ke																																																		
> Platform Key (PK)	862																																																				
> Key Exchange Keys	1560																																																				
> Authorized Signatures	3143																																																				
> Forbidden Signatures	10588	220	Factory																																																		
> Authorized TimeStamps	0	0	No Keys																																																		
> OsRecovery Signatures	0	0	No Keys																																																		

Version 2.20.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
Key Exchange Keys	see box

8.5.1.1.9 Authorized Signatures

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th colspan="4" style="text-align: center;">Authorized Signatures</th> </tr> <tr> <td colspan="4" style="text-align: center;">Details</td> </tr> <tr> <td colspan="4" style="text-align: center;">Export</td> </tr> <tr> <td colspan="4" style="text-align: center;">Update</td> </tr> <tr> <td colspan="4" style="text-align: center;">Append</td> </tr> <tr> <td colspan="4" style="text-align: center;">Delete</td> </tr> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Secure Boot variable</th> <th style="width: 10%;">Size</th> <th style="width: 10%;">Ke</th> <th style="width: 50%;">Factory</th> </tr> </thead> <tbody> <tr> <td>> Platform Key (PK)</td> <td>862</td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td>1560</td> <td></td> <td></td> </tr> <tr> <td>> Authorized Signatures</td> <td>3143</td> <td></td> <td></td> </tr> <tr> <td>> Forbidden Signatures</td> <td>10588</td> <td>220</td> <td>Factory</td> </tr> <tr> <td>> Authorized TimeStamps</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> <tr> <td>> OsRecovery Signatures</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> </tbody> </table>	Authorized Signatures				Details				Export				Update				Append				Delete				Secure Boot variable	Size	Ke	Factory	> Platform Key (PK)	862			> Key Exchange Keys	1560			> Authorized Signatures	3143			> Forbidden Signatures	10588	220	Factory	> Authorized TimeStamps	0	0	No Keys	> OsRecovery Signatures	0	0	No Keys	<p>Enroll Factory Defaults or load certificates from a file:</p> <ol style="list-style-type: none"> 1.Public Key Certificate: <ol style="list-style-type: none"> a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image (SHA256) <p>Key Source: Factory, External, Mixed</p> <hr/> <p>←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
Authorized Signatures																																																					
Details																																																					
Export																																																					
Update																																																					
Append																																																					
Delete																																																					
Secure Boot variable	Size	Ke	Factory																																																		
> Platform Key (PK)	862																																																				
> Key Exchange Keys	1560																																																				
> Authorized Signatures	3143																																																				
> Forbidden Signatures	10588	220	Factory																																																		
> Authorized TimeStamps	0	0	No Keys																																																		
> OsRecovery Signatures	0	0	No Keys																																																		

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
Authorized Signatures	see box

8.5.1.1.10 Forbidden Signatures

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th colspan="4" style="text-align: center;">Forbidden Signatures</th> </tr> <tr> <td colspan="4" style="text-align: center;">Details</td> </tr> <tr> <td colspan="4" style="text-align: center;">Export</td> </tr> <tr> <td colspan="4" style="text-align: center;">Update</td> </tr> <tr> <td colspan="4" style="text-align: center;">Append</td> </tr> <tr> <td colspan="4" style="text-align: center;">Delete</td> </tr> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Secure Boot variable</th> <th style="width: 10%;">Size</th> <th style="width: 10%;">Ke</th> <th style="width: 50%;">Factory</th> </tr> </thead> <tbody> <tr> <td>> Platform Key (PK)</td> <td>862</td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td>1560</td> <td></td> <td></td> </tr> <tr> <td>> Authorized Signatures</td> <td>3143</td> <td></td> <td></td> </tr> <tr> <td>> Forbidden Signatures</td> <td>10588</td> <td>220</td> <td>Factory</td> </tr> <tr> <td>> Authorized TimeStamps</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> <tr> <td>> OsRecovery Signatures</td> <td>0</td> <td>0</td> <td>No Keys</td> </tr> </tbody> </table>	Forbidden Signatures				Details				Export				Update				Append				Delete				Secure Boot variable	Size	Ke	Factory	> Platform Key (PK)	862			> Key Exchange Keys	1560			> Authorized Signatures	3143			> Forbidden Signatures	10588	220	Factory	> Authorized TimeStamps	0	0	No Keys	> OsRecovery Signatures	0	0	No Keys	<p>Enroll Factory Defaults or load certificates from a file:</p> <ol style="list-style-type: none"> 1.Public Key Certificate: <ol style="list-style-type: none"> a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image (SHA256) <p>Key Source: Factory, External, Mixed</p> <hr/> <p>←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</p>
Forbidden Signatures																																																					
Details																																																					
Export																																																					
Update																																																					
Append																																																					
Delete																																																					
Secure Boot variable	Size	Ke	Factory																																																		
> Platform Key (PK)	862																																																				
> Key Exchange Keys	1560																																																				
> Authorized Signatures	3143																																																				
> Forbidden Signatures	10588	220	Factory																																																		
> Authorized TimeStamps	0	0	No Keys																																																		
> OsRecovery Signatures	0	0	No Keys																																																		

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
Forbidden Signatures	see box

8.5.1.1.11 Authorized TimeStamps

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr> <th colspan="4" style="text-align: center;">Authorized TimeStamps</th> </tr> <tr> <td style="width: 30%;"></td> <td style="width: 10%; text-align: center;">Update</td> <td style="width: 10%; text-align: center;">Append</td> <td style="width: 50%;"></td> </tr> <tr> <td>Secure Boot variable</td> <td style="text-align: center;">Size</td> <td style="text-align: center;">Ke</td> <td></td> </tr> <tr> <td>> Platform Key (PK)</td> <td style="text-align: center;">862</td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td style="text-align: center;">1560</td> <td style="text-align: center;">1</td> <td>Factory</td> </tr> <tr> <td>> Authorized Signatures</td> <td style="text-align: center;">3143</td> <td style="text-align: center;">2</td> <td>Factory</td> </tr> <tr> <td>> Forbidden Signatures</td> <td style="text-align: center;">10588</td> <td style="text-align: center;">220</td> <td>Factory</td> </tr> <tr> <td>> Authorized TimeStamps</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> <td>No Keys</td> </tr> <tr> <td>> OsRecovery Signatures</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> <td>No Keys</td> </tr> </table>	Authorized TimeStamps					Update	Append		Secure Boot variable	Size	Ke		> Platform Key (PK)	862			> Key Exchange Keys	1560	1	Factory	> Authorized Signatures	3143	2	Factory	> Forbidden Signatures	10588	220	Factory	> Authorized TimeStamps	0	0	No Keys	> OsRecovery Signatures	0	0	No Keys	<p>Enroll Factory Defaults or load certificates from a file:</p> <p>1.Public Key Certificate:</p> <p>a)EFI_SIGNATURE_LIST</p> <p>b)EFI_CERT_X509 (DER)</p> <p>c)EFI_CERT_RSA2048 (bin)</p> <p>d)EFI_CERT_SHAXXX</p> <p>2.Authenticated UEFI Variable</p> <p>3.EFI PE/COFF Image (SHA256)</p> <p>Key Source:</p> <p>Factory,External,Mixed</p> <hr/> <p>←: Select Screen</p> <p>↑↓: Select Item</p> <p>Enter: Select</p> <p>+/-: Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Reset</p> <p>ESC: Exit</p>
Authorized TimeStamps																																					
	Update	Append																																			
Secure Boot variable	Size	Ke																																			
> Platform Key (PK)	862																																				
> Key Exchange Keys	1560	1	Factory																																		
> Authorized Signatures	3143	2	Factory																																		
> Forbidden Signatures	10588	220	Factory																																		
> Authorized TimeStamps	0	0	No Keys																																		
> OsRecovery Signatures	0	0	No Keys																																		

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
Authorized TimeStamps	see box

8.5.1.1.12 OsRecovery Signatures

Aptio Setup - AMI
Security

<p>Vendor Keys Modified</p> <p>Factory Key Provision [Disabled]</p> <p>> Restore Factory Keys</p> <p>> Reset To Setup Mode</p> <p>> Export Secure Boot variables</p> <p>> Enroll Efi Image</p> <p>Device Guard Ready</p> <p>> Remove 'UEFI CA' from DB</p> <p>> Restore DB defaults</p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr> <th colspan="4" style="text-align: center;">OsRecovery Signatures</th> </tr> <tr> <td style="width: 30%;"></td> <td style="width: 10%; text-align: center;">Update</td> <td style="width: 10%; text-align: center;">Append</td> <td style="width: 50%;"></td> </tr> <tr> <td>Secure Boot variable</td> <td style="text-align: center;">Size</td> <td style="text-align: center;">Ke</td> <td></td> </tr> <tr> <td>> Platform Key (PK)</td> <td style="text-align: center;">862</td> <td></td> <td></td> </tr> <tr> <td>> Key Exchange Keys</td> <td style="text-align: center;">1560</td> <td style="text-align: center;">1</td> <td>Factory</td> </tr> <tr> <td>> Authorized Signatures</td> <td style="text-align: center;">3143</td> <td style="text-align: center;">2</td> <td>Factory</td> </tr> <tr> <td>> Forbidden Signatures</td> <td style="text-align: center;">10588</td> <td style="text-align: center;">220</td> <td>Factory</td> </tr> <tr> <td>> Authorized TimeStamps</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> <td>No Keys</td> </tr> <tr> <td>> OsRecovery Signatures</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> <td>No Keys</td> </tr> </table>	OsRecovery Signatures					Update	Append		Secure Boot variable	Size	Ke		> Platform Key (PK)	862			> Key Exchange Keys	1560	1	Factory	> Authorized Signatures	3143	2	Factory	> Forbidden Signatures	10588	220	Factory	> Authorized TimeStamps	0	0	No Keys	> OsRecovery Signatures	0	0	No Keys	<p>Enroll Factory Defaults or load certificates from a file:</p> <p>1.Public Key Certificate:</p> <p>a)EFI_SIGNATURE_LIST</p> <p>b)EFI_CERT_X509 (DER)</p> <p>c)EFI_CERT_RSA2048 (bin)</p> <p>d)EFI_CERT_SHAXXX</p> <p>2.Authenticated UEFI Variable</p> <p>3.EFI PE/COFF Image (SHA256)</p> <p>Key Source:</p> <p>Factory,External,Mixed</p> <hr/> <p>←: Select Screen</p> <p>↑↓: Select Item</p> <p>Enter: Select</p> <p>+/-: Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Reset</p> <p>ESC: Exit</p>
OsRecovery Signatures																																					
	Update	Append																																			
Secure Boot variable	Size	Ke																																			
> Platform Key (PK)	862																																				
> Key Exchange Keys	1560	1	Factory																																		
> Authorized Signatures	3143	2	Factory																																		
> Forbidden Signatures	10588	220	Factory																																		
> Authorized TimeStamps	0	0	No Keys																																		
> OsRecovery Signatures	0	0	No Keys																																		

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Vendor Keys	None
OsRecovery Signatures	See box

8.6 Boot

```

Aptio Setup - AMI
Main  Advanced  Chipset  Security  Boot  Save & Exit

Boot Configuration
Setup Prompt Timeout          1
Bootup NumLock State         [On]

F7 Boot Menu                   [Enabled]
Quiet Boot                     [Enabled]

StartUpDelay for UEFI shell    5

FIXED BOOT ORDER Priorities
Boot Option #1                 [Service Stick]
Boot Option #2                 [CFast]
Boot Option #3                 [SSD]
Boot Option #4                 [HDD]
Boot Option #5                 [CD/DVD]
Boot Option #6                 [USB Stick]
Boot Option #7                 [USB Floppy]
Boot Option #8                 [USB Hard Disk]
Boot Option #9                 [USB CD/DVD]
Boot Option #10                [Network]
Boot Option #11                [USB Lan]

▶ Advanced Fixed Boot Order Parameters

Number of seconds to wait for
setup activation key.
65535 (0xFFFF) means indefinite
waiting

←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Reset
ESC: Exit

Version 2.22.1282 Copyright (C) 2024 AMI
    
```

BIOS entry	Options
Boot Configuration	
Setup Prompt Timeout	None
Bootup NumLock State	On / Off
F7 Boot Menu	Disabled / Enabled
Quiet Boot	Enabled / Disabled
Fixed Boot Order Priorities	
Boot Option #1-11	Specify the order of the boot media to be used.
Advanced Fixed Boot Order Parameters	Submenu: Advanced Fixed Boot Order Parameters ▶ 82

8.6.1 Advanced Fixed Boot Order Parameters

Aptio Setup - AMI		
Boot		
Min. CFAST capacity (GB)	0	Lower capacity limit for boot group CFAST in GB
Max. CFAST capacity (GB)	119	
Min. SSD capacity (GB)	119	
Max. SSD capacity (GB)	481	
Min. HDD capacity (GB)	481	
Max. HDD capacity (GB)	8000000	
Max. USB Stick capacity (GB)	64	
UEFI BDS Boot Filter	[Enabled]	
Re-enable UEFI Disks	[Enabled]	
BootDeviceDef Version 3(11/22/2018)		
Version 2.22.1282 Copyright (C) 2024 AMI		

BIOS entry	Options
Min. CFAST capacity	None
Max. CFAST capacity	None
Min. SSD capacity (GB)	None
Max. SSD capacity (GB)	None
Min. HDD capacity (GB)	None
Max. HDD capacity (GB)	None
Max. USB Stick capacity (GB)	None
UEFI BDS Boot Filter	Enabled / Disabled
Re-enable UEFI Disks	Enabled / Disabled
BootDeviceDef Version 3(11/22/2018)	None

8.7 Save & Exit

Aptio Setup - AMI

Main Advanced Chipset Security Boot **Save & Exit**

Save Changes and Reset Discard Changes and Reset Restore Optimized Defaults Boot Override Launch EFI Shell from filesystem device	Reset the system after saving the changes. ←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
---	--

Version 2.22.1282 Copyright (C) 2024 AMI

BIOS entry	Options
Save Changes and Reset	Press enter key
Disacrd Changes and Reset	Press enter key
Restore Optimized Defaults	Press enter key
Boot Override	None
Launch EFI Shell from filesystem device	Press enter key

8.8 BIOS update

The "DecdFlsh" program and a bootable medium with the latest BIOS version are used if the BIOS needs to be updated. When doing this it is important to start the program from a DOS environment without a virtual memory manager such as "EMM386.EXE". If such a memory manager is loaded, the program will abort with an error message or cause a crash.

DecdFlsh is a program for the automatic updating of the BIOS on all boards with AMI-BIOS. All files contained in the zip file must be unpacked into a directory, from where

```
DecdFlsh Bios-Dateiname
```

calling takes place. The name of the BIOS file and its length are checked. The BIOS will now be programmed.

The system must not be interrupted during the flashing process, as otherwise the update will abort and the BIOS on the board will be destroyed. The Flash procedure takes about 75 seconds. The necessary firmware update takes place automatically.

NOTICE

Risk of damage due to incorrect update procedure!

If the BIOS update is performed incorrectly, the board may become unusable. Therefore a BIOS update should only be done if the corrections / additions that the new BIOS version brings with it are really needed.

Before a planned BIOS update, it is essential to ensure that the BIOS file to be reloaded is really released for exactly this board and for exactly this board version. If an inappropriate file is used, the board will inevitably not boot afterwards.

9 LEDs

The LEDs for the status messages of the CB8283 motherboard are provided on the C9900-A083 LED board. This is screwed onto the housing cover. The connection to the board is made with a cable via the 4-pin connector (P100). The power supply of the board is (3.3 V). The LEDs are described from left to right.

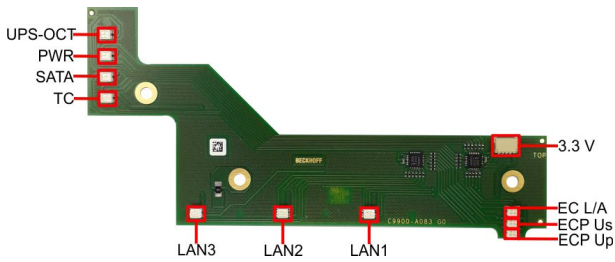


Fig. 10: LED board

9.1 LED: UPS-OCT

The RGB LED indicates the transmission quality of the UPS-OCT signals by means of colors and flashing intervals.

Color	Interval	Meaning
None	Steadily lit	No UPS-OCT connected
Blue	Flashing	Bootloader active
Yellow	Steadily lit	Moderate signal quality
Green	Steadily lit	Good signal quality
Red	Steadily lit	Poor signal quality

If the LED is not lit, no UPS-OCT is connected.

i Adaptation of the status codes

It is possible to adapt the status codes (e.g. as UPS-OCT-LED). To do this, the system colors can be changed with the aid of an SMB command. This change remains in force until the next restart or reset.

9.2 LED: PWR

The RGB LED indicates status messages of the power controller by means of colors and flashing intervals.

Color	Interval	Meaning
None	Steadily lit	PC is off / system in error state
White	Steadily lit	Powerfail
Cyan	Steadily lit	Reserved
Magenta	Steadily lit	S UPS active (if present)
Blue	Steadily lit	Reserved
Yellow	Steadily lit	S5 state, Windows shut down, supply voltage still present
Green	Steadily lit	S0 state, normal operation
Red	Steadily lit	Reset/Start
Green/yellow	Flashing	Bootloader running without error
Red/yellow	Flashing	Bootloader is starting (start sequence is being run through)
Yellow	Flashing (6 s)	S4 state
Yellow	Flashing (3 s)	S3 state
Magenta	Flashing (0.5 s)	S UPS capacitance test (if S UPS present)
Red/magenta	Flashing	Checksum error during I ² C transmission in the bootloader

A steadily lit red LED can indicate a hardware error.

9.3 LED: SATA

The RGB LED indicates the hard disk activity.

Color	Interval	Meaning
Red	Flashing	Activity (access to storage medium)

9.4 LED: TwinCAT

The RGB LED indicates status messages for TwinCAT by means of colors and flashing intervals.

Color	Interval	Meaning
Green	Steadily lit	TwinCAT Run Mode
Blue	Steadily lit	TwinCAT Config Mode
Red	Steadily lit	TwinCAT Stop
-	-	TwinCAT not started

i Adaptation of the status codes

It is possible to adapt the status codes (e.g. as TwinCAT LED). To do this, the system colors can be changed with the aid of an SMB command. This change remains in force until the next restart or reset. A change of the default colors is indicated by the additional flashing of the white LED.

9.5 LED: LAN 1 - LAN 3

The LEDs of the LAN interfaces indicate the activity and speed of the data transmission (Mbit/s). The LEDs light up during connection and flash during data transmission:

LED Permanently on when connected	LED Flashing during data transmission	Mbit/s
White	White	2500
Green	Green	1000
Orange	Orange	100/10



The LEDs directly on the interface are not visible with existing wiring. Their signals are forwarded to the display on the housing via an additional LED board.

9.6 EtherCAT LEDs

These LEDs indicate the various statuses of the EtherCAT P connection.

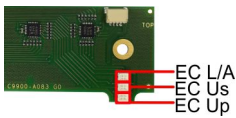


Fig. 11: EtherCAT P LEDs

LED	Color/flashing interval	Meaning
EC L/A	green on	Connection to the network (1000 Mbit/s)
	green flashing	Data transmission running (1000 Mbit/s)
EC L/A	orange on	Connection to the network (100 Mbit/s)
	orange flashing	Data transmission running (100 Mbit/s)
ECP U _s	green on	System voltage in normal range (24 V)
	red on	Voltage outside the normal range
ECP U _p	green on	Peripheral voltage in normal range (24 V)
	red on	Voltage outside the normal range

9.7 Power supply LED board

The LED board is supplied with a voltage of 3.3 V via a 4-pin plug.

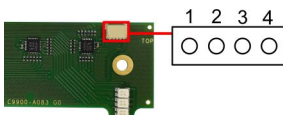


Fig. 12: Power supply LED board

Pin assignment power supply plug		
Pin	Name	Description
1	3.3 V	Voltage 3.3 V +
2	SCLK	Serial Clock Signal
3	SDAT	Serial DATA Signal
4	GND	Ground

10 Mechanical drawing



Dimensions

Dimensions in mil, millimeters are in square brackets [mm].

10.1 Printed circuit board: dimensions and holes

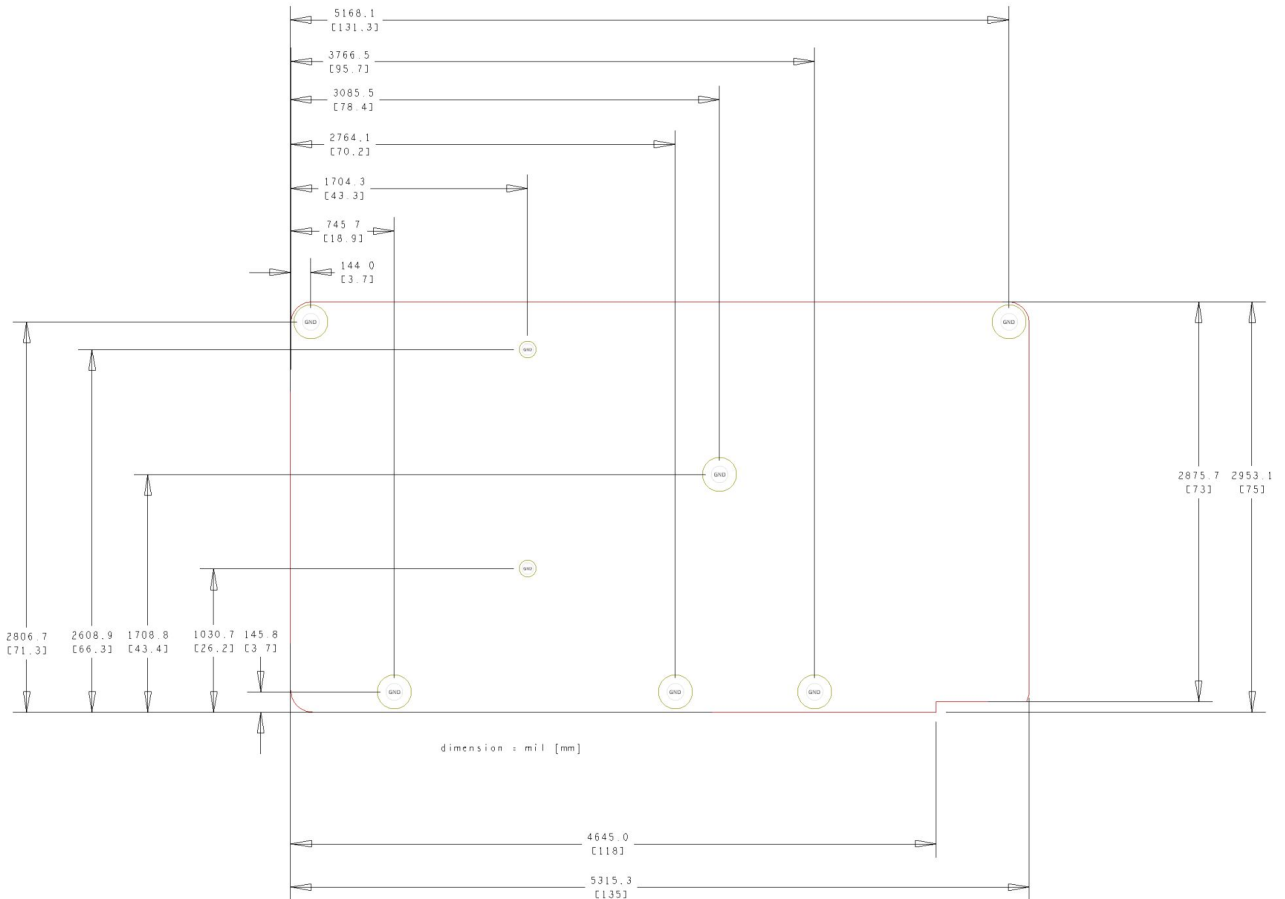


Fig. 13: CB8283 MZ

11 Technical data

11.1 Electrical data

Power supply	
Board	24 V _{DC} (+20 % / -15 %)
RTC	≥3 A

Power	
Transformer	30 W continuous load 60 W peak load

Current consumption	
RTC	≤10 μA

11.2 Environmental conditions

Temperature range	
Operating	0 °C ... +50 °C (extended temperature range on request)
Storage	-25 °C ... +85 °C
Shipping	-25 °C ... +85 °C, for packed boards

Temperature changes	
Operating	0.5 °C per minute, 7.5 °C in 30 minutes
Storage	1.0 °C per minute
Shipping	1.0 °C per minute, for packed boards

Relative humidity	
Operating	5 % ... 85 % (non-condensing)
Storage	5 % ... 95 % (non-condensing)
Shipping	5 % ... 100% (non-condensing), for packed boards

Impact	
Operating	150 m/s ² , 6 ms
Storage	400 m/s ² , 6 ms
Shipping	400 m/s ² , 6 ms, for packed boards

Vibrations	
Operating	10 ... 58 Hz, amplitude 0.075 mm 58 to 500 Hz, 10 m/s ²
Storage	5 ... 9 Hz, amplitude 3.5 mm 9 to 500 Hz, 10 m/s ²
Shipping	5 ... 9 Hz, amplitude 3.5 mm 9 to 500 Hz, 10 m/s ² , for packed boards

i Note on impact and vibration resistance

The specifications for impact and vibration resistance refer only to the motherboard itself without heat sink, memory module, cabling, etc.

11.3 Thermal specifications

The board is specified for an ambient temperature range of 0 °C to +50 °C (extended temperature range on request). In addition, care must be taken that the temperature of the processor die does not exceed 110 °C. To ensure this a suitable cooling concept must be implemented that is oriented to the maximum power consumption of the processor/chipset. It must also be ensured that any existing controllers are included in the cooling concept. The power consumption of these function blocks may be of the same order of magnitude as the power consumption of the processor.

The board is prepared with suitable holes for the use of modern cooling solutions. We have a series of compatible cooling components in our range. Your distributor will be pleased to assist you in selecting suitable solutions.

NOTICE

Prevent the maximum die temperature being exceeded!

It is the end customer's responsibility to ensure that the die temperature of the processor does not exceed 110 °C! Continuous overheating can destroy the board!

If the temperature exceeds 110 °C, the ambient temperature needs to be reduced. Ensure sufficient air circulation if necessary.

12 Appendix I: Post Codes

During the boot phase, the BIOS generates a series of status messages (so-called "POST Codes"), which can be output with the help of a suitable reading device (POST Code card). The meanings of the POST Codes are explained in the document "Aptio™ 5.x Status Codes" from American Megatrends®, which is available from the website <http://www.ami.com>. In addition, the following OEM POST Codes are output:

Code	Description
87h	BIOS-API started
88h	PCA9535 started
89h	PWRCTRL firmware started

13 Appendix II: Resources

13.1 Interrupt

The resources used depend on the setup setting. The listed interrupts and their use are given by the AT compatibility. If interrupts are to be available only on the ISA side, they must be reserved by the BIOS setup. Exclusivity on the PCI side is neither given nor possible.

13.2 PCI-Devices

The PCI devices listed here all exist on the board, including those that are detected and configured by the BIOS. Due to the BIOS setup settings it may be the case that various PCI devices or functions of devices are not activated. If devices are disabled, the bus numbers of other devices may change as a result.

Bus	Dev.	Fct.	Controller / Slot
00	00	00	Host Bridge ID 3E30
00	01	00	PCI-to- PCI Bridge ID1901
00	01	01	PCI-to- PCI Bridge ID1905
00	01	02	PCI-to- PCI Bridge ID1909
00	02	00	VGA Controller ID3E98
00	08	00	System Device ID1911
00	12	00	Data Acquisition/Signal Processing Controller ID A379
00	14	00	XHCI USB Controller ID A36D
00	14	02	RAM Controller ID A36F
00	16	00	Communication Device ID A360
00	16	03	Serial Device ID A363
00	17	00	RAID Controller ID 2822
00	1D	00	PCI-to-PCI Bridge ID A330
00	1D	04	PCI-to-PCI Bridge ID A334
00	1F	02	ISA Bridge ID A306
00	1F	03	HD Audio Device ID A348
00	1F	04	SMBus Controller ID A323
00	1F	05	Controller ID A324
00	1F	06	Ethernet Controller ID 15BB
01	00	00	Ethernet Controller (PCIE) ID 1533
02	00	00	Ethernet Controller (PCIE) ID 1533
03	00	00	Ethernet Controller (PCIE) ID 1533

13.3 SMB-Devices

The following table lists the reserved SM-Bus device addresses in 8-bit notation.

NOTICE

These address ranges may not be used by external devices even if the component assigned in the table doesn't exist on the motherboard.

Address	Function
34-35	API access to power supply
36-39	Reserved
5C-5D	NCT7491
60-6F	Reserved for DDR4
70-73	POST-Code Output
88-89	Slave address defined by BIOS
A0-A7	Reserved for DDR4
B0-B3	Power controller (access via BIOS-API)
B8-BB	Power controller (access via BIOS-API)

14 Support and Service

Beckhoff and their partners around the world offer comprehensive support and service, making available fast and competent assistance with all questions related to Beckhoff products and system solutions.

Download finder

Our [download finder](#) contains all the files that we offer you for downloading. You will find application reports, technical documentation, technical drawings, configuration files and much more.

The downloads are available in various formats.

Beckhoff's branch offices and representatives

Please contact your Beckhoff branch office or representative for [local support and service](#) on Beckhoff products!

The addresses of Beckhoff's branch offices and representatives round the world can be found on our internet page: www.beckhoff.com

You will also find further documentation for Beckhoff components there.

Beckhoff Support

Support offers you comprehensive technical assistance, helping you not only with the application of individual Beckhoff products, but also with other, wide-ranging services:

- support
- design, programming and commissioning of complex automation systems
- and extensive training program for Beckhoff system components

Hotline: +49 5246 963-157
e-mail: support@beckhoff.com

Beckhoff Service

The Beckhoff Service Center supports you in all matters of after-sales service:

- on-site service
- repair service
- spare parts service
- hotline service

Hotline: +49 5246 963-460
e-mail: service@beckhoff.com

Beckhoff Headquarters

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20
33415 Verl
Germany

Phone: +49 5246 963-0
e-mail: info@beckhoff.com
web: www.beckhoff.com

Trademark statements

Beckhoff®, TwinCAT®, TwinCAT/BSD®, TC/BSD®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® and XPlanar® are registered trademarks of and licensed by Beckhoff Automation GmbH.

Third-party trademark statements

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc and any use of such marks by Beckhoff is under license.

Intel, the Intel logo, Intel Core, Xeon, Intel Atom, Celeron and Pentium are trademarks of Intel Corporation or its subsidiaries.

Microsoft, Microsoft Azure, Microsoft Edge, PowerShell, Visual Studio, Windows and Xbox are trademarks of the Microsoft group of companies.

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Germany
Phone: +49 5246 9630
info@beckhoff.com
www.beckhoff.com