



# **K1 and K2 POS Motherboard**

**(with UEFI BIOS Setup)**

**User Manual (Edition November 2018)**

We would like to know your opinion on this publication.  
Please send us a copy of this page if you have any constructive criticism.  
We would like to thank you in advance for your comments.

With kind regards,

---

**Your opinion:**

Diebold Nixdorf Systems GmbH  
Documentation R&D BLN  
Wohlrabedamm 31  
D-13629 Berlin  
E-Mail: [retail.documentation@dieboldnixdorf.com](mailto:retail.documentation@dieboldnixdorf.com)  
Order No.: **01750266921B**

# **K1 and K2 POS Motherboard**

User Manual

Edition November 2018

All brand and product names mentioned in this document are trademarks of their respective owners.

**Copyright © Diebold Nixdorf Systems GmbH, 2018**

The reproduction, transmission or use of this document or its contents is not permitted without express authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility model or design, are reserved. Delivery subject to availability; technical modifications possible.

# Contents

<b>Contents</b> .....	<b>1</b>
<b>Overview</b> .....	<b>4</b>
Introduction .....	4
Some Highlights of the K1 and K2 Motherboard .....	4
<b>Motherboard Specification</b> .....	<b>5</b>
Block Diagram .....	5
Internal Connectors .....	6
Mainboard assembly variants .....	7
CPU support .....	7
Mainboard internal connectors and onboard features .....	7
Serial ports (internal).....	7
USB 2.0 (internal) .....	8
Mini PCI Express .....	9
Memory (internal).....	10
SATA (internal) .....	10
Fan (internal).....	10
Chassis intrusion connector (internal).....	11
Front panel connector (internal).....	11
ATX / 12V Power connector (internal) .....	12
LPT (internal) .....	13
TPM .....	13
PCI Express Slots (internal) .....	14
Mainboard onboard connectors with external access .....	15
Motherboard I/O shield overview (external) .....	15
PanelLink 2.0 (external).....	15
VGA (external) .....	18
Keyboard / Mouse (external) .....	18
LAN (external).....	18
USB 2.0 / USB 3.0 (external) .....	18
Audio (external).....	18
<b>Technical Data</b> .....	<b>19</b>
Supported Sleep States.....	20
RAID (K1 Motherboard) .....	21

<b>Changing the Battery</b> .....	<b>22</b>
<b>UEFI BIOS Setup</b> .....	<b>23</b>
Standard UEFI BIOS Version .....	23
BIOS Menu Bar .....	24
Legend Screen .....	24
General Help .....	25
Scroll Bar .....	25
Info Screen .....	26
Main Menu.....	28
Advanced Menu .....	29
Sub Menu ➤ ACPI Settings .....	29
Sub Menu ➤ Trusted Computing.....	30
TPM 1.2.....	30
TPM 2.0.....	31
Sub Menu ➤ Hardware Configuration.....	33
Sub Menu ➤ CPU Configuration .....	37
Sub Menu ➤ SATA Configuration .....	40
Sub Menu ➤ PCH-FW Configuration .....	41
Sub Menu ➤ AMT Configuration .....	43
Sub Menu ➤ USB Configuration .....	45
Sub Menu ➤ NTC6106D Super IO Configuration.....	47
Sub Menu ➤ NTC6106D H/W Monitor .....	48
Sub Menu ➤ Intel TXT Information .....	48
Sub Menu ➤ Serial Port Console Redirection .....	49
Sub Menu ➤ Network Stack Configuration .....	51
Sub Menu ➤ CMOS.....	51
Sub Menu ➤ Intel(R) Ethernet Network Connection .....	52
Chipset Menu.....	53
Sub Menu ➤ PCH-IO Configuration .....	53
Sub Menu ➤ PCH-IO Conf. ➤ BIOS Security Configuration .....	53
Sub Menu ➤ System Agent (SA) Configuration .....	54
Boot Menu .....	56
Security Menu .....	58
Sub Menu ➤ Secure Boot menu.....	59
Save & Exit Menu .....	60
Test Points Codes .....	61
Checkpoint Ranges .....	61
SEC Phase.....	62
PEI Phase .....	62

PEI Beep Codes .....	65
DXE Phase.....	65
DXE Beep Codes .....	68
<b>Abbreviations .....</b>	<b>69</b>

# Overview

## Introduction

This manual describes the features of two variants of a Motherboard based on the Intel 8 series chipset Q87 and H81, formerly known as Lynx Point.

## Some Highlights of the K1 and K2 Motherboard

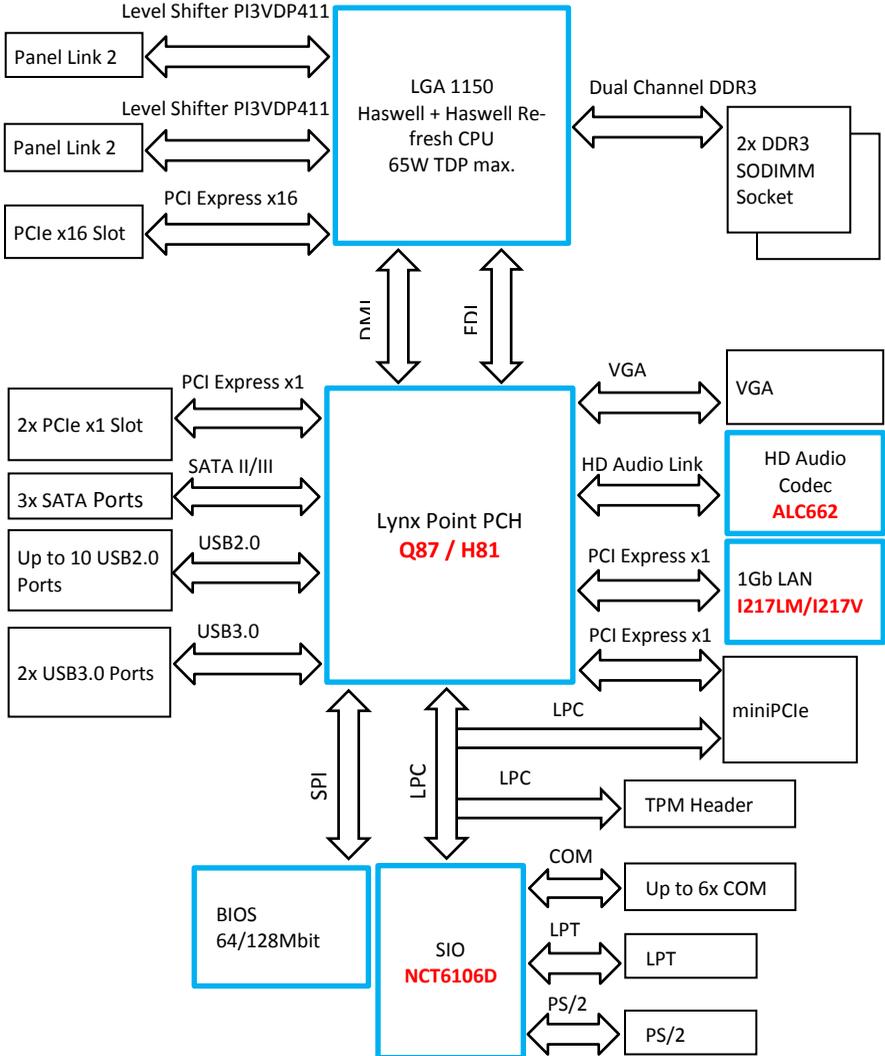
- 4th Generation Intel® Core™ Processors, formerly known as Haswell
- Intel 8 series chipset Q87 and H81, formerly known as Lynx Point
- CPU integrated graphic controller up to Intel® HD Graphics 4600, depending on used processor
- AMT 9.1 support at K1 motherboards
- 2x Panellink 2 interfaces
- 1x VGA interface
- Gigabit LAN onboard (Intel® Ethernet Connection; Q87: I217-LM, H81: I217-V)
- 3 SATA ports (Q87: 3xSATA III, H81: 2x SATA III + 1x SATA II)
- 2x DDR3 SODIMM sockets, supporting up to 16GB (2x8GB) at 1600MHz. Only ~3GB available for 32bit OS
- 1x PCI Express x16 gen3
- 2x PCI Express x1 gen2
- 6 COM ports. COM1 is unpowered, COM2-6 have the option to be powered
- 1 LPT port
- MiniPCIe socket (full size) supporting the WN NVRAM module
- 2 USB3.0 ports
- up to 10 USB2.0 ports (H81: 6 ports)



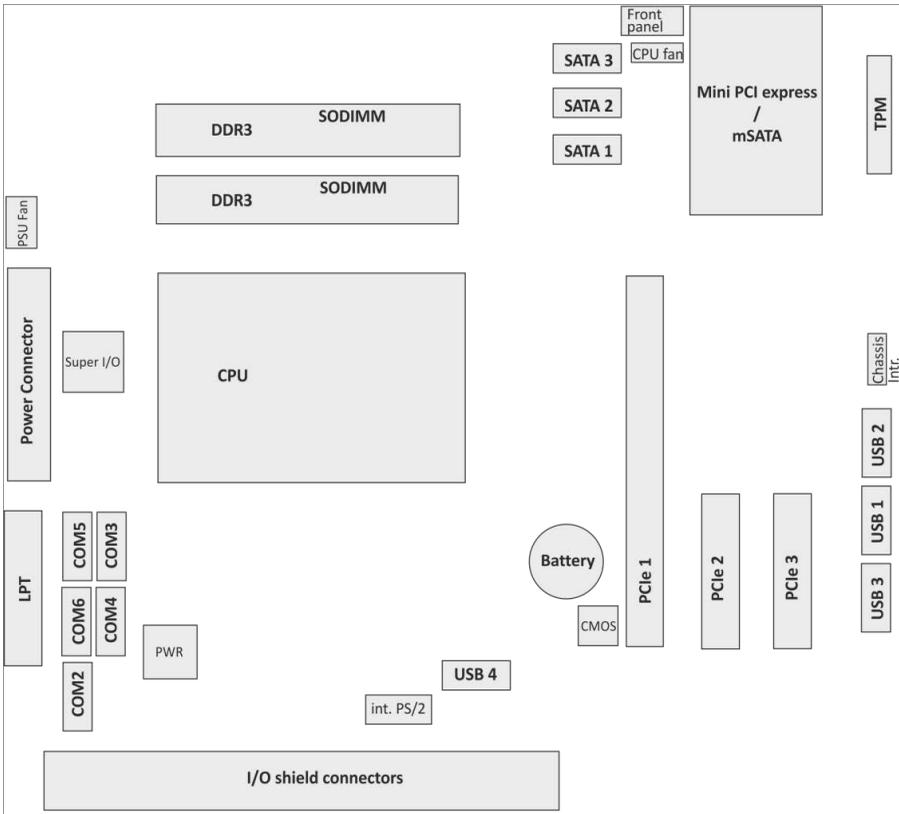
TFT- displays without DDC are not supported.

# Motherboard Specification

## Block Diagram



# Internal Connectors



## Mainboard assembly variants

As mentioned above there are two motherboard variants: The **K1** board with Q87 chipset supporting AMT and RAID and the **K2** board with H81 chipset as value edition supporting lesser features.

## CPU support

CPU	CPU#	#CPU core	#Threads	GHz Core	GHz GFX	Cache size	TDP [W]
i5	i5-4570TE	2	4	2.7 (3.3)	0.35 (1)	4MB	35
i5	i5-4570S	4	4	2.9 (3.6)	0.35(1.15)	6MB	65
i3	i3-4330TE	2	4	2.4	0.35 (1)	4MB	35
i3	i3-4330	2	4	3.5	0.35 (1.15)	4MB	54
Pentium	G3320TE	2	2	2.3	0.35 (1)	3MB	35
Pentium	G3420	2	2	3.2	0.35 (1.15)	3MB	53
Celeron	G1820TE	2	2	2.2	0.35 (1)	2MB	35
Celeron	G1820	2	2	2.7	0.35 (1.05)	2MB	53

## Mainboard internal connectors and onboard features

### Serial ports (internal)

COM2 -6 are configurable to standard or powered COM ports with an internal COM cable option (max current for powered COM: single port 300mA@5V; all ports together not more than 500mA@5V; single port 600mA@12V; all ports together not more than 900mA@12V).

Maximum voltage drop on 12V is 300mV, on 5V it is 150mV at full load. This output is designed according to UL regulations and is protected by a self-resettable fuse.

COM1 is a standard 9 pin DSUB connector in I/O shield supporting “WAKE On Ring” functionality.

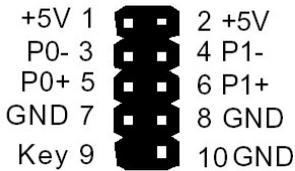
2x 6 pin header, 2.54 mm pitch

Pin	Signal
1	DCD
2	RX
3	TX
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI
10	Key Pin
11	+5 V
12	+12 V



### USB 2.0 (internal)

8 USB ports at K1 board and 4 USB ports at K2 are routed to 10pin double row headers with 2.54 mm pitch. Each header provides 2 ports. These headers are intended to connect optional front USB modules or USB hubs.



Two USB ports share one fuse. USB port 11 at header USB3 (pins 1,3,5,7) is shared with PCIe x1 connector PCIE3 (pins A5 to A8) for USB uplink connection for the "Retail Card".

## Mini PCI Express

The mainboard provides a full size mini PCI Express (rev.1.1) / mSATA connector. It is placed on top, thus being accessible without removing other components. It supports LPC signals including serial interrupts. Auto detection by mSATA presence detect supports automated switch between mSATA and PCIe functionality (PCIe functionality only supported in conjunction with Q87 chipset according to mini PCI Express Standard Rev 1.1). The **K1 motherboard** supports PCIe **and** mSATA functionality, the **K2 motherboard** supports mSATA functionality only.

**Connector type:** Standard MiniPCIe 1.1 connector full size

Pin	Function	Pin	Function
1	WAKE	2	VCC3
3	n.c.	4	GND
5	n.c.	6	VCC 1.5V
7	CLKRQ#	8	FRAME#
9	GND	10	LAD3
11	REFCLK-	12	LAD2
13	REFCLK+	14	LAD1
15	GND	16	LAD0
17	SUSCLK 32KHz	18	GND
19	CLK 33MHz	20	n.c.
21	GND	22	RESET#
23	PCIE_RX- / SATA +B	24	3VSB
25	PCIE_RX+ / SATA -B	26	GND
27	GND	28	VCC 1.5V
29	GND	30	SMB_CLK
31	PCIE_TX- / SATA -A	32	SMB_DATA
33	PCIE_TX+ / SATA +A	34	GND
35	GND	36	n.c. (USB-)
37	GND	38	n.c. (USB+)
39	VCC3	40	GND
41	VCC3	42	n.c.
43	GND	44	n.c.
45	n.c.	46	n.c.
47	n.c.	48	VCC 1.5V
49	n.c.	50	GND
51	mSATA presence detect	52	VCC3

## Memory (internal)

The mainboard provides two DDR3 SODIMM sockets supporting up to 16GB in dual channel mode. The horizontal mounting of the SODIMM sockets ensures an optimal air flow.

## SATA (internal)

The mainboard provides three standard SATA ports. The ports SATA1 (white) and SATA2 (blue) supporting SATA III connectivity speed. Port SATA3 (black) supports SATA III speed at K1 board, and SATA II speed at K2 board. The RAID functionality is only supported by the K1 motherboard.

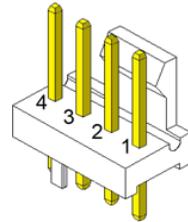
## Fan (internal)

The mainboard provides two fan connectors. The CPU fan connector supports PWM fans with 4 pin connection.

Connector details are: 2.54mm (.100") Pitch Vertical Header, with Friction Lock, 4 (3) Circuits, PC Tail Length: 3.50mm (.138"). Molex Part Nr: 47053-1000 or similar. The connector follows the Intel "4-Wire Pulse Width Modulation (PWM) Controlled Fans" specification.

### PWM Fan

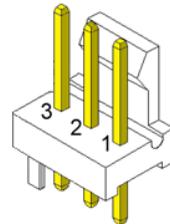
Pin	Signal	Signal Description
1	GND	GND
2	12 V	Fan operation voltage
3	Sense	Tachometric signal
4	Control	PWM control signal (only 4 pin connector)



The PSU fan connector has 3 pin connection with DC fan speed regulation.

### DC Fan

Pin	Signal	Signal Description
1	GND	GND
2	PWR	Operation Voltage 6-12 V
3	Sense	Tachometric signal



### Chassis intrusion connector (internal)

The mainboard supports a chassis intrusion connector.

Type: 3 pin shrouded header, B3B-PH-K-S (JST) or equivalent.

Pin Number	Function
1	GND
2	Intrusion input (switch to GND if chassis is open)
3	n.c.



### Front panel connector (internal)

The mainboard supports a front panel connector to support service elements (like POWER ON pushbutton, HDD and power LEDs).

The Power LED at the chassis front connected to this front panel header is green when system is powered on (S0). During Stand By (S3) it blinks green and when system is in hibernation (S4) or powered down (S5) the LED is orange.

Power Status	Power LED
S0	Green
S3	Green blinking
S4, S5	Orange

The BIOS is able to disable the power button. This feature is automatically enabled when "Follow AC power" is selected within the BIOS setup. Then it is not possible to switch off the system by the power button, even when pressed longer than 4s. But when the OS is shut down correctly, system can be switched on again by the power button.

The front panel header also supports speaker connection.

Type: 2x6 pin header, 2.54 mm pitch.

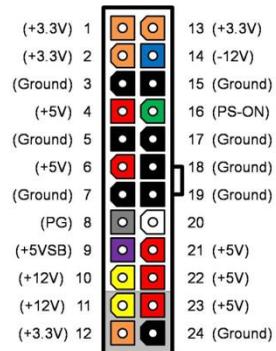
Pin Number	Function
1	Power switch +
2	Reset switch +
3	Power switch -
4	Reset switch -
5	Power LED +
6	Speaker -
7	Power LED -
8	Coding
9	HDD LED +
10	GND
11	HDD LED -
12	Speaker +



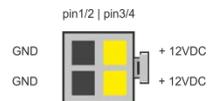
### ATX / 12V Power connector (internal)

The mainboard provides a 4 pin and a 24 pin ATX power connector.

Pin Number	Function
1,2,12,13	+3.3V
3,5,7,15,17,18,19,24	GND
4,6,21,22,23	+5V
8	Power ok
9	5V SB
10, 11	+12V
14	-12V
16	PS-ON
20	n.c.



Pin Number	Function
1,2	GND
3,4	+12V



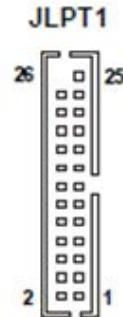
A 20 pin ATX power cable can be plugged into the 24 pin connector on the motherboard, too. In this case the pins 11,12,23 and 24 are not used and

left open. The 4 pin ATX power connector has to be connected to the PSU anyway, otherwise the motherboard will not work.

### LPT (internal)

Connector type: 26 pin shrouded header, 2.54mm pitch

Pin	Function	Pin	Function
1	STR#	14	GND
2	AFD#	15	D6
3	D0	16	GND
4	ERR#	17	D7
5	D1	18	GND
6	PINIT#	19	ACK#
7	D2	20	GND
8	LPT_SLIN#	21	BUSY
9	D3	22	GND
10	GND	23	PE
11	D4	24	GND
12	GND	25	SLCT
13	D5	26	Key

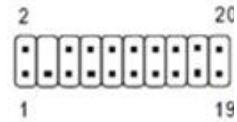


### TPM

The mainboard supports one dedicated TPM port. This connector slot is placed on top and is accessible without removing any other components.

Connector type: pin header RM2.54

Pin	Function	Pin	Function
1	CLK	11	LDA0
2	GND	12	GND
3	LFRAME	13	Reserved
4	Key (no pin)	14	Reserved
5	LRESET	15	3V SB
6	VCC 5V	16	SERIRQ
7	LAD3	17	GND
8	LAD2	18	CLKRUN
9	VCC3	19	LPCPD
10	LAD1	20	Reserved



### PCI Express Slots (internal)

There are two PCIe slots x1 and one 1 PCIe slot x16.

Use in **BEETLE /MIII** systems

Only low profile cards are supported.

Height 68.90 mm (2.731 inches) maximum,  
Length 167.65 mm (6.600 inches) maximum

PCIe cards are able to wake up the system.

Thermal management: The input power of a single PCIe x1 card must not exceed 10W and x16 card does not exceed 30W.

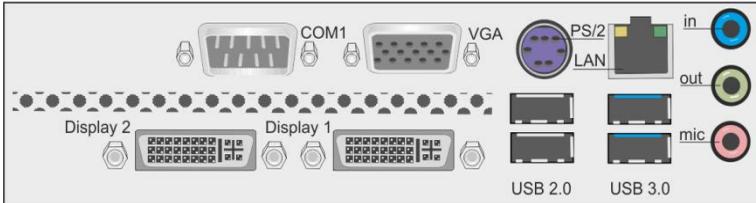
The PCIe slot at the outer side of the mainboard supports USB signals on PCIe pins A5 (D-) and A8 (D+) as USB uplink connection and A6+A7 (VBUS) to Retail specific PCIe card.

The same USB port is routed to the USB3 connector.

## Mainboard onboard connectors with external access

### Motherboard I/O shield overview (external)

The picture below shows the arrangement of the onboard I/O connectors.



### PanelLink 2.0 (external)

The PanelLink 2.0 interface is based on a DVI-I connector and uses DVI-D signals. There is no analog VGA connection even if it is a DVI-I connector. Unused pins of the connector are connected to USB signals.

## Pin assignment

Pin	DVI-D	Function PL2.0
1	TMDS Data 2-	TMDS Data 2-
2	TMDS Data 2+	TMDS Data 2+
3	TMDS Data shield	TMDS Data shield
4	n.c.	+12V
5	n.c.	+12V
6	DDC CLK	DDC CLK
7	DDC DATA	DDC DATA
8	n.c. (VSYNC)	Power button RMT
9	TMDS Data 1-	TMDS Data 1-
10	TMDS Data 1+	TMDS Data 1+
11	TMDS Data shield	TMDS Data shield
12	n.c.	+12V
13	n.c.	+12V
14	5V	+5V SB
15	GND	GND
16	Hotplug detect	Hotplug detect
17	TMDS Data 0-	TMDS Data 0-
18	TMDS Data 0+	TMDS Data 0+
<b>PIN</b>	<b>DVI-D</b>	<b>Function PL2.0</b>
19	TMDS Data shield	TMDS Data shield
20	n.c.	+12V
21	n.c.	+12V
22	TMDS Data shield	TMDS Data shield
23	TMDS CLK+	TMDS CLK+
24	TMDS CLK-	TMDS CLK-
C1	n.c. (red)	
C2	n.c. (green)	GND
C3	n.c. (Blue)	USB-
C4	n.c. (HSYNC)	USB+
C5	GND	GND

The +12V signals are protected by a self-resettable fuse and are able to deliver a current of 2.5A.

This voltage rail is only enabled if a monitor DDC identification is passed and a PL2-capable monitor was detected, e.g. vendor ID is Diebold Nixdorf (05dh 0d8h) and device ID is in the range of 30000...34999.

This output is designed according to UL regulations as limited power output. This output is switched off when PL2 connector is removed and is only switched on again after PL2 connector was attached and DDC identification detected a supported monitor again.

5VSB (pin 14) supply is enabled in S3, S4 and S5.

RMT pin 8 is a low active input and represents an ACPI button. This button supports system wakeup and system sleep functionality. It does not immediately power down the system if it is pressed for longer than 4s (power button overwrite).

The RMT feature is only supported by Display 1 connector.

### VGA (external)

This interface uses a 15 pin DSUB connector in the upper row of I/O shield. Sync signals VSYNC and HSYNC have 5V logic high level.

### Keyboard / Mouse (external)

The Keyboard/Mouse connector is a part of the motherboard I/O shield. It also supports mouse and keyboard connection simultaneously by using a PS/2 Y-cable.

### LAN (external)

The mainboard supports 1Gbit connection to a Local Area Network (LAN). Indication **LED** for link and activity is available.

Right LED	Speed Indication
10mbit	off
100mbit	green
1000mbit	orange

Left LED	Link&Activity
Link at every speed	Yellow on
Traffic at every speed	Yellow blinking

WOL (wake on LAN) and PXE are supported.

### USB 2.0 / USB 3.0 (external)

Four USB ports (two for USB2.0 and two for USB3.0) are located in the mainboard I/O connector area.

### Audio (external)

The mainboard supports a microphone-in, a line-out and a line-in connector in I/O shield. The connector type is stereo 3.5mm diameter.

# Technical Data

Topic	Remarks
Form Factor	µATX 226x210mm
Processor	4th Generation Intel® Core™ Processors
Chipset	Intel Series 8 ( <b>K1</b> : Q87; <b>K2</b> : H81)
CPU Socket	LGA1150
Graphics	Celeron 1820: Intel HD Graphics Core i3: Intel HD 4600 Core i5: Intel HD 4600
Main Memory	Dual channel memory architecture 2 sockets supporting unbuffered non-ECC DDR3 memory modules supporting up to 16GB system memory SODIMM
Storage	3x SATA III (K1) 2x SATA III + 1x SATA II (K2) RAID support (K1 only)
LAN	onboard Gigabit LAN, status LED activity and link
Audio	Realtek HD audio Codec ALC 662
PS/2	Mouse and keyboard (PS/2) connector onboard in I/O shield
USB	2x USB 3.0 10x USB 2.0 (K1) 6x USB 2.0 (K2)
Expansion Slots	2x PCIe x1 1x PCIe x16 slot 1x MiniPCIe 1.1 (used by <b>K1</b> only), additional LPC signals 1x TPM slot
Motherboard External I/O Connectors (at I/O Shield)	2x Plink2.0 / DVI-D 1x LAN (RJ45) + 2x USB3.0 1x PS/2 + 2x USB2.0 1x VGA 1x COM <b>Audio:</b> Line in (blue) Line out (green) Microphone in (pink)

Internal I/O Connectors	4x USB 2.0 headers supporting 2 ports each (K1) 2x USB 2.0 headers supporting 2 ports each (K2) 1x PCIe x16 2x PCIe x1 1x MiniPCIe, v1.1 2x DDR3 SODIMM 3x SATA 1x CPU fan 4pin 1x PSU fan 3pin 5x COM header 1x LPT header 1x Chassis intrusion 1x 24pin ATX 1x 4pin ATX 1x TPM header 1x PS/2 header 1x Front panel header
Other Special Features	1x CMOS clear jumper
Product Lifecycle	5 years without changing OS software driver critical components e.g. audio codec, LAN, Super-I/O, Chipset
AMT	Version 9.1 at K1 board only



### Hardware Monitor

The requirements for the hardware monitoring are described in the BIOS chapter Hardware Monitor.

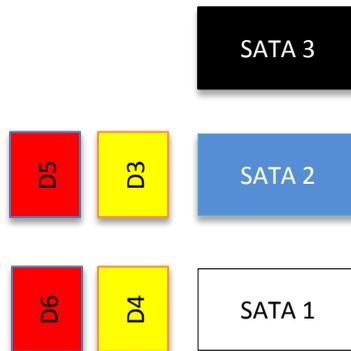
## Supported Sleep States

S0	Normal Operation (“ON”)
S3	Suspend to RAM / “Stand By”
S4	Suspend to Disk / “Hibernation”
S5	Soft Off

## RAID (K1 Motherboard)

The K1 motherboard provides RAID functionality for the SATA interface. Raid level 0 (striping), 1 (mirroring) and 5 (striping with distributed parity) are supported. For RAID 5 three HDD/SSD devices are needed. To enable the RAID functionality please see the corresponding chapter in the BIOS setup description.

For SATA ports 1 and 2 there are onboard LEDs indicating the status of the attached HDD/SSD within the RAID Array. The functionality of the SATA LEDs depends on host software (Intel SATA/RAID driver (“Rapid Storage Technology” – driver at the time of writing)). The host software needs to be installed and running for LED indication to work.



LED	Color	Function
D3	Yellow	Read/Write activity indication for SATA2 port
D4	Yellow	Read/Write activity indication for SATA1 port
D5	Red	Failure indication for SATA2 port
D6	Red	Failure indication for SATA1 port

# Changing the Battery

The systems are equipped with a lithium battery on the motherboard to ensure data retention, the time and the setup parameters. The battery should be changed approximately every five years.



When inserting the new battery, make sure the polarity is correct. This is marked in the socket. Incorrect replacement of the battery may lead to the danger of explosion.

The battery is located in a socket on the Motherboard. To gain access to the battery, proceed as described in the according chapters of your **BEETLE User Manual**.



The lithium battery must be replaced only by identical batteries or types recommended by Diebold Nixdorf.

You can return the used batteries to your Diebold Nixdorf sales outlet. Batteries containing harmful substances are marked accordingly.

The chemical denotations are as follows: **CD** = Cadmium; **Pb** = Lead, **Li** = Lithium.



This symbol on a battery tells you that batteries containing harmful substances must not be disposed of as household waste. Follow the country specific laws and regulations. Within the  European Union you are legally bound to return these batteries to the service organization where you purchased the new battery.



The setup parameters must be reset each time the battery has been changed.

# UEFI BIOS Setup

The mainboard K1.x-Q87-uATX-STD and K2.x-H81-uATX-STD comes with an AMI UEFI BIOS chip that contains the ROM Setup information of your system. This chip serves as an interface between the processor and the rest of the mainboard's components. This section explains the information contained in the Setup program and tells you how to modify the settings according to your system configuration.

Even if you are not prompted to use the Setup program, you might want to change the configuration of your system in the future. For example, you may want to enable the Security Password Feature or make changes to the power management settings. It will then be necessary to reconfigure your system using the BIOS Setup program so that the system can recognize these changes and record them in the NVRAM. All setup data is stored in a non-volatile memory (NVRAM). When you remove the battery, all parameters will be lost.

## Standard UEFI BIOS Version

The UEFI BIOS ROM of the system holds the Setup utility. When you turn on the system, it will provide you with the opportunity to run this program. This appears during the Power-On Self-Test (POST). Press <F2> to call the Set-up utility. If you missed the opportunity to pressing the mentioned key, POST will continue with its test routines, thus preventing you from calling Setup. If you still need to call Setup, reset the system by pressing <Ctrl> + <Alt> + <Del>. You can also restart by turning the system off and then on again. But do so only if the first method fails.

If you like to change the boot order only once, you can press the <F10> key during the POST is running. At the end you will see a Pop-Up window with all the devices the system has found. With the keys <UP> and <DOWN> you select the boot device.

The Setup program has been designed to make it as easy as possible. It is a menu-driven program, which means you can scroll through the various sub-menus and make your selections among the predetermined choices. When you invoke Setup, the main program screen will appear. Read more about the Setup entries on the following pages.

Because the UEFI BIOS software is constantly being updated, the following UEFI BIOS screens and descriptions are for reference purposes only and may not reflect your UEFI BIOS screens exactly.

## BIOS Menu Bar

The top of the screen has a menu bar with the following sections:

Info	Use this menu for information only
Main	Use this menu to make changes to the basic system configuration.
Advanced	Use this menu to enable and make changes to the advanced features.
Chipset	Use this menu to configure the chipset specific options
Boot	Use this menu to configure the default system device used to locate and load the Operating System.
Security	Use this menu to enable a supervisor or user password and Intrusion Detection.
Save & Exit	Use this menu to exit the current menu or specify how to exit the Setup program.



To access the menu bar items, press the right or left arrow key on the keyboard until the desired item is highlighted.

## Legend Screen

The right frame displays the key legend. The keys in the legend frame allow you to navigate through the various setup menus. The following table lists the keys found in the legend with their corresponding alternates and functions.

<b>Navigation Key(s)</b>	<b>Description of Functions</b>
← or → (keypad arrows)	Select the menu item to the left or right.
↑ or ↓ (keypad arrows)	Moves the highlight up or down between fields.
Enter	Move into sub menu or change selected menu items
+ (plus key) - (minus key)	Change field contents.
<Tab>	Jumps from one field to the next.
<F1>	Opens a general Help Screen with extended information.
<F2>	Load previous values (Load last saved values)
<F3>	Load optimized values (Factory reset)
<F4>	Saves changes and exits Setup.
<Esc>	Opens a windows to select between exit and return to setup

## General Help

In addition to the Item Specific Help window, the UEFI BIOS setup program also provides a General Help screen. This screen can be called from any menu by simply pressing <F1>. The General Help screen lists the legend keys with their corresponding alternates and functions.

## Scroll Bar

When a scroll bar appears to the right of a help window, it indicates that there is more information to be displayed that will not fit in the window. Use <PgUp> and <PgDn> or the up and down keys to scroll through the entire help document.

Press <Home> to display the first page, press <End> to reach the last page. To exit the help window, press the <Enter> or <Esc> key.

## Sub-Menu



Note that a right pointer symbol “>” appears left of certain fields. This pointer indicates that a sub-menu can be launched from this field. A sub-menu contains additional options for a field parameter.

To call a sub-menu, simply move the highlight to the field and press <Enter>. The sub-menu then will appear immediately. Use the legend keys to enter values and move from field to field within a sub-menu just as you would do within a menu. Use the <Esc> key to return to the main menu.

Take some time to familiarize yourself with each of the legend keys and their corresponding functions. Practice navigating through the various menus and sub-menus. If you accidentally make unwanted changes to any of the fields, use the set default hot key <F3>. While moving around through the Setup program, note that explanations appear in the Item Specific Help window located to the right side of each menu. This window displays the help text for the currently highlighted field.

## Info Screen

When the Setup program is accessed, the following info screen appears:

```
..... Info Page
Product Name:                K#. #-###-uATX-STD
Bios Version:                xx/yy
Bios Date:                   MM/DD/YYYY
Ethernet MAC-Address:        AC-DC-FA-DE-BE-EF
UUID:
d716af80-6f0a-1018-8789-fbd248a1242f
System:
-----
###-----
Mainboard:
-----
-----
Power Supply:
-----
-----
```

This screen is for information only. There is nothing that could be changed within Setup. All information is intended to facilitate the support of your system.

**Product Name:**

This text is fixed for your mainboard with standard UEFI BIOS. This board is also called "K1.x-Q87-uATX-STD" or "K2.x- H81-uATX-STD"

**BIOS Version:**

The UEFI BIOS version is displayed in the WN release format xx/yy

The UEFI BIOS Date is displayed the date of release in international format: MM/DD/YYYY

**Ethernet MAC Address:**

The Ethernet MAC-Address of the on board LAN Controller is displayed at this line if this device is enabled.

**UUID Info:**

A UUID is an identifier standard used in software construction, standardized by the Open Software Foundation. The intent of UUIDs is to enable distributed systems to uniquely identify information without significant central coordination.

**System, Main board, Power Supply:**

The default placeholders may be replaced by specific data from factory, describing configuration, serial number etc. for each device.

## Main Menu

BIOS Information	
Bios Vendor	American Megatrends
Compliance	UEFI 2.3.1; PI 1.2
Total Memory	2048 MB (DDR3)
Memory Frequency	1333 MHz
System Date	[Mo 07/07/2014]
System Time	[23:23:23]
Processor and Chipset Information	

### System Date [MM/DD/YYYY]

Set your system to the date that you specify (usually the current date). The format is month, day, year. Valid values for month, day and year are:  
Month: (1 to 12), Day (1 to 31), Year: (up to 2079).

### System Time [XX: XX: XX]

Set your system to the time that you specify (usually the current time). The format is hour, minute, second. Valid values for hour, minute, and second are: Hour: (00 to 23), Minute: (00 to 59), Second: (00 to 59). Press <Enter> to terminate every entry value and reach the next position. On the upper right frame find the keys listed to modify the values.

### Processor and Chipset Information

This enters a Sub-Menu with summaries of used processor and chipset.

## Advanced Menu

- ACPI Settings
- Trusted Computing
- Hardware Configuration
- CPU Configuration
- SATA Configuration
- PCH-FW Configuration
- AMT Configuration
- USB Configuration
- NCT6106D Super IO Configuration
- NCT6106D HW Monitor
- Intel TXT Information
- Serial Port Console Redirection
- Network Stack Configuration
- CMOS
  
- Intel(R) Ethernet Network Connection
- Driver Health

### Sub Menu ➤ ACPI Settings

- ACPI Settings
  
- Enable ACPI Auto Configuration [Enabled]

### Enable ACPI Auto Configuration **[Enabled]**

Being an ACPI BIOS system, the operating system is allowed to control the Power Management features of the computer and the setting for Advanced Power Management (APM) BIOS mode are ignored.

Not all operating systems support ACPI BIOS mode.

Configuration options: [Disabled] [Enabled].

## Sub Menu ► Trusted Computing

The mainboard can be upgraded with a TPM module, either according to TCG standard 1.2 or 2.0. Accordingly, two different TPM configurations are displayed.

### TPM 1.2

Configuration	
Security Device Support	[Disable]
TPM State	[Disabled]
Pending Operation	[None]
Current Status Information	
TPM Enabled Status	[Disabled]
TPM Active Status	[Deactivated]
TPM Owner Status	[Unowned]
No security device found	

#### **Security Device Support** **[Disable]**

This option enables or disables the Trusted Platform Module.

After change this option the system will reboot automated.

If the security device is disabled the OS will not show this device in device list.

Configuration options: [Disable] [Enable].

#### **TPM State** **[Disabled]**

This option changes the actual state of the security module.

Select the TPM operation after the next automated reboot of the system.

Configuration options: [Disabled] [Enabled].

#### **Pending operation** **[None]**

[None]: The TPM state will be untouched.

[Clear]: This option resets the TPM module after the next automated reboot of the system.

**Attention!** All data and keys of the TPM module are permanently deleted and can no longer be restored.

## TPM 2.0

TPM20 Device Found	
Vendor: IFX	
Firmware Version: 5.63	
Security Device Support	[Enable]
Active PCR banks	SHA-1,SHA256
Available PCR banks	SHA-1,SHA256
SHA-1 PCR Bank	[Enabled]
SHA256 PCR Bank	[Enabled]
Pending operation	[None]
Platform Hierarchy	[Enabled]
Storage Hierarchy	[Enabled]
Endorsement Hierarchy	[Enabled]
TPM2.0 UEFI Spec Version	[TCG_2]
Physical Presence Spec Version	[1.3]
TPM 20 InterfaceType	[TIS]

### **Security Device Support** **[Enabled]**

This option enables or disables the Trusted Platform Module.

After change this option the system will reboot automated.

If the security device is disabled the OS will not show this device in device list.

### **SHA-1 PCR Bank** **[Enabled]**

Enable or Disable SHA-1 PCR Bank

**SHA256 PCR Bank** **[Enabled]**

Enable or Disable SHA256 PCR Bank.

**Pending operation [None]**

[None]: The TPM state will be untouched.

[Clear]: This option resets the TPM module after the next automated re-boot of the system.

**Attention!** All data and keys of the TPM module are permanently deleted and can no longer be restored.

**Platform Hierarchy** **[Enabled]**

Enable or Disable Platform Hierarchy.

**Storage Hierarchy** **[Enabled]**

Enable or Disable Storage Hierarchy.

**Endorsement Hierarchy** **[Enabled]**

Enable or Disable Endorsement Hierarchy.

**TPM2.0 UEFI Spec Version** **[TCG\_2]**

Select the TCG2 Spec Version Support, TCG\_1\_2: the Compatible mode for Win8/Win10, TCG\_2: Support new TCG2 protocol and event format for Win10 or later.

**Physical Presence Spec Version** **[1.3]**

Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.

## Sub Menu ➤ Hardware Configuration

PCH LAN Controller	[Enabled]
Launch PXE OpROM policy	[Legacy only]
Wake On LAN	[Disabled]
Wake On Ring	[Disabled]
Wake On Time	[Disabled]
Wake On USB/PS2 (S3)	[Enabled]
Wake On LAN S3	[Disabled]
Wake On PCIe Slot	[Disabled]
RMT Button Display1	[Enabled]
RMT Button Display2	[Disabled]
Display Output to COM	[Disabled]
Restore AC Power Loss	[Power Off]
BootOrder Menu	[Enabled]
VT-d	[Enabled]

### **PCH LAN Controller** [Enabled]

This option allows enabling or disabling the on-board LAN controller.  
Configuration options: [Disabled] [Enabled].

### **Launch PXE OpROM policy** [Legacy only]

Preboot Execution Environment (PXE) refers a method to boot up over network without the need for a hard drive or boot diskette.  
Configuration options: [Do not launch] [UEFI only] [Legacy only].

### **Wake On LAN** [Disabled]

This allows enabling or disabling power up the BEETLE when the LAN controller receives a call while the BEETLE is in Soft-Off or Hibernate mode.  
Configuration options: [Disabled] [Enabled].

### **Wake On Ring** [Disabled]

This allows enabling or disabling power up the BEETLE when the modem receives a call while the BEETLE is in Soft-Off or Hibernate mode.



The BEETLE cannot receive or transmit data until the system and applications are fully running, thus connection cannot be made on the first try. Turning an external modem off and then back on while the BEETLE is off causes an initialization string that will cause the system to power on.

Configuration options: [Disabled] [Enabled].

### **Wake On Time**

**[Disabled]**

This allows enabling or disabling power up the BEETLE on specific time while the system is in Soft-Off or Hibernate mode. If this option is enabled a wake time is programmable within next two lines. The first line is setting the hour in international format (0-23). The second line is setting the minutes (0-59).

Configuration options: [Disabled] [Enabled].



Wake time is also adjustable from OS and can override this option.

### **Wake On USB/PS2 (S3)**

**[Enabled]**

This allows enabling or disabling power up the BEETLE when a USB- or a PS2- Keyboard/Mouse receives a call while the BEETLE is in Soft-Off mode.

Configuration options: [Disabled] [Enabled] [Auto].

### **Wake On PCIe Slot**

**[Disabled]**

This allows enabling or disabling power up the BEETLE when a device mounted in a PCIe slot receives a call while the BEETLE is in Soft-Off mode.

Configuration options: [Disabled] [Enabled].

### **Wake On LAN (S3)**

**[Disabled]**

Enable or Disable wakeup system via LAN while the system is in S3. If set to [Auto] it will follow OS related settings.

Configuration options: [Disabled] [Enabled].

### **Wake-on Modes**

Please note that you have to shut down the system in power saving modes by OS before you can use Wake-on modes. Switching off the system by main power switch or front button-override will not initialize system

wakeup functions. See following table, which wakeup events are available from different power states:

	Standby (S3)	Hibernate (S4)	Soft off (S5)
Front Button	Yes	Yes	Yes
LAN	Yes (Note5)	Yes (Note1)	Yes (Note1)
Modem (Note2)	Yes	Yes	Yes
USB/PS2 (Note3)	Yes	No	No
PCIe Slot (Note4)	Yes	Yes	Yes

Note 1: “Yes” is valid only, if the option <Wake on LAN> is [Enabled].

Note 2: “Yes” is valid only, if the option <Wake on Ring> is [Enabled].

Note 3: “Yes” is valid only, if the option <Wake on USB/PS2> is [Enabled].

Note 4: “Yes” is valid only, if the option <Wake on PCIe Slot> is [Enabled].

Note 5: “Yes” is valid only, if the option <Wake on LAN S3> is [Enabled].

**RMT Button Display1** **[Enabled]**

This option enables or disables the power button of connected BA9x display at DVI port 1 to switch on/off the BEETLE system.

Configuration options: [Disabled] [Enabled].

**Display Output to COM** **[Disabled]**

This option enables or disables the display output control to a device connected to COM2 – COM6.

Configuration options: [Disabled] [COM2] [COM3] [COM4] [COM5] [COM6].

**Restore AC Power Loss** **[Power Off]**

Select the options to reboot the system after power has been interrupted.

[Power off] leaves the system off until pressing the power button.

[Last State] reboots the system automatically if it was active before

power loss. [Follow AC Power] will start up anytime power is available.

The front button will be disabled to prevent an accidental shutdown.

It’s not possible to force a shutdown by pressing the front button for more than four seconds.

Configuration options: [Power off] [Last State] [Follow AC Power].

**Power Button****[Auto]**

If this option is [Disabled] the power button is locked when system is running. If this option is set to [Auto] the power button is locked only if the option Restore AC Power Lost is set to [Follow AC Power] Configuration options: [Disabled] [Enabled] [Auto].

**Bootorder Menu****[Enabled]**

This option enables or disables the popup menu to change the boot order by pressing F10 during POST.

[Enabled] Popup menu is available during POST

[Disabled] Popup menu is not available during POST

**VT-d****[Enabled]**

Check to enable VT-d function on MCH

Configuration options: [Disabled] [Enabled].

## Sub Menu ➤ CPU Configuration

Items marked with ‘\*’ are not available by all Intel processors

CPU Configuration	
Intel (R) Core (TM) i3-4330TE CPU	
2.40GHz	
Hyper Threading	[Enabled]
Active Processor Core	[All]
Overclocking lock	[Disabled]
Limit CPUID Maximum	[Disabled]
Execute Disable Bit	[Enabled]
Intel Virtualization Technology	[Enabled]
Hardware Prefetcher	[Enabled]
Adjacent Cache Line Prefech	[Enabled]
CPU AES	[Enabled]
Boot performance mode	[Max Non-Turbo Per....]
EIST	[Enabled]
Turbo Mode*	[Enabled]
Intel TXT(LT) Support	[Disabled]
➤ CPU Configuration Parameters	

### Hyper-threading

[Enabled]

This option allows enabling or disabling the Intel(R) Hyper-threading Technology to uses processor resources more efficiently, enabling multiple threads to run on each core.

Configuration options: [Disabled] [Enabled].

### Active Processor Cores

[All]

This option enables all or several cores of an Intel processor.

The numbers of cores are depends of used processor type.

Configuration options: [All] [Number of cores 1-x].

**Overclocking lock****[Disabled]**

This option enables or disables the overclocking feature of an Intel processor.

Configuration options: [Disabled] [Enabled].

**Limit CPUID Maximum****[Disabled]**

When CPUID instruction is executed, newer CPU may return a value greater than 3 which cause a certain problem with specific operating systems. Enabling "Limit CPUID Maximum" will limit the returned value to 3 (and less) to get rid of the problem. The problem does not occur with Windows series operating systems.

Configuration options: [Disabled] [Enabled]

**Execute Disable Bit****[Enabled]**

Execute Disable Bit (EDB) is an Intel© Hardware-based security feature that can help reduce system exposure to viruses and malicious code. EDB allows the processor to classify areas in memory where application code can or cannot execute.

Configuration options: [Disabled] [Enabled]

**Intel Virtualization Technology****[Enabled]**

Virtualization enhanced by Intel© Virtualization Technology will allow a system to run multiple operating systems and applications in independent partitions. With virtualization, one computer system can function as multiple "virtual" systems.

Configuration options: [Disabled] [Enabled]

**Hardware Prefetcher****[Enabled]**

The processor has a hardware prefetcher that automatically analyses its requirements and prefetches data and instructions from the memory into the Level 2 cache. This reduces the latency associated with memory reads.

Configuration options: [Disabled] [Enabled]

**Adjacent Cache Line Prefetch****[Enabled]**

The processor has a hardware adjacent cache line prefetch mechanism that automatically fetches an extra 64-byte cache line whenever the processor requests for a 64-byte cache line. This reduces cache latency by making the next cache line immediately available if the processor requires it as well.

Configuration options: [Disabled] [Enabled]

**CPU AES \*****[Enabled]**

This option enables or disables the CPU Advanced Encryption Standard instructions.

Configuration options: [Disabled] [Enabled]

**Boot performance mode****[Max Non-Turbo Performance]**

This option adjusts the performance of Boot mode.

Configuration options: [Max Non-Turbo Performance] [Max Battery] [Turbo Performance]

**EIST****[Enabled]**

This option enables or disables the Enhanced Intel SpeedStep Technology of an Intel processor.

Configuration options: [Disabled] [Enabled].

**Intel TXT (LT) Support \*****[Disabled]**

Intel Trusted Execution Technology (TXT) is supported by several Intel processors.

Configuration options: [Disabled] [Enabled]

## Sub Menu ➤ SATA Configuration

SATA Controllers	[Enabled]
SATA Mode selection	[AHCI]
Aggressive LPM Support	[Enabled]
SATA Controller Speed	[Auto]
SATA 0 (white)	Emty
Hot Plug	[Disabled]
Spin Up Device	[Disabled]
SATA 1 (blue)	Emty
Hot Plug	[Disabled]
Spin Up Device	[Disabled]
SATA 4 (mSATA)	Emty
Hot Plug	[Disabled]
Spin Up Device	[Disabled]
SATA 5 (black)	Emty
Hot Plug	[Disabled]
Spin Up Device	[Disabled]

### **SATA Controller(s)** **[Enabled]**

This option enables or disables the SATA controller.

Configuration options: [Disabled] [Enabled].

### **SATA Mode selection** **[AHCI]**

This option selects the SATA controller mode. The option [RAID] is only available on K1 boards with Q87 Chipset.

Configuration options: [AHCI] [IDE] [RAID].

Following two menu items are only available if SATA Mode selection is set to AHCI:

### **Aggressive LPM Support** **[Enabled]**

This option enables or disables the PCH to aggressively enter link power state. This is only supported under AHCI mode.

Configuration options: [Disabled] [Enabled].

### SATA Controller Speed

[Auto]

This option **indicates** the maximum speed the SATA Controller can support.

### SATA 0, 1, 5

If option SATA Controller(s) is enabled SATA ports 0, 1 and 5 can handle hard disks and CD-, DVD- or Blu-ray devices. For each port are following options available if AHCI mode is enabled:

Hot Plug [Disabled] [Enabled]

Spin Up Device [Disabled] [Enabled]

### SATA 4

SATA port 4 is an mSATA port which cannot handle hard disks and CD-, DVD- or Blu-ray devices.

## Sub Menu ➤ PCH-FW Configuration

ME FW Version	9.1.1.1000
ME Firmware Mode	Normal Mode
ME Firmware Type	Full Sku Firmware
ME Firmware SKU	5MB
NFC Capability State	[Disabled]
MEBx Type	[None]
MDES BIOS State Code	[Disabled]
➤ Firmware Update Configuration	

## Intel ME (Management Engine) Subsystem

Intel ME (Management Engine) Subsystem is a separated microcontroller embedded in the chipset driven by a special firmware. For systems with K1 mainboard the ME handles an own setup and can be entered while booting the system by pressing the keys CTRL + P.

**MEBx Type** **[None]**

This option is only available on K2 boards with H81 chipset and selects the type of MEBx.

Configuration options: [None] [miniMEBx]

**MDES BIOS State Code** **[Disabled]**

This option enables or disables the MDES BIOS State Code.

Configuration options: [Disabled] [Enabled]

➤ **Firmware Update Configuration**

ME FW Image Re-Flash [Disabled]

This option enables or disables the ME FW Image Re-Flash.

Configuration options: [Disabled] [Enabled]

## Sub Menu ➤ AMT Configuration

Intel® Active-Management-Technology is a technology for remotely managing and securing PCs out-of-band. Intel AMT is only available at K1 mainboards.

Intel AMT	[Enabled]
BIOS Hotkey Pressed	[Disabled]
MEBx Selection Screen	[Disabled]
Hide Un-Configure ME Confirmation	[Disabled]
MEBx Debug Message Output	[Disabled]
Un-Configure ME	[Disabled]
AMT Wait Timer	0
Disable ME	[Disabled]
ASF	[Enabled]
Activate Remote Assistance Process	[Disabled]
USB Configure	[Disabled]
PET Progress	[Enabled]
AMT CIRA Timeout	0
WatchDog	[Disabled]
OS Timer	0
BIOS Timer	0

### Intel AMT **[Enabled]**

Intel Active Management Technology (AMT) is a special firmware to maintenance the system with remote systems. This option enables or disables the AMT. All other options are not available if AMT is disabled.  
Configuration options: [Disabled] [Enabled]

### BIOS Hotkey Pressed **[Disabled]**

This option enables or disables the BIOS hotkey press.  
Configuration options: [Disabled] [Enabled]

### MEBx Selection Screen **[Disabled]**

This option enables or disables the MEBx selection screen.  
Configuration options: [Disabled] [Enabled]

- Hide Un-Configure ME Confirmation** **[Disabled]**  
This option hides Un-Configure ME without password confirmation prompt. Configuration options: [Disabled] [Enabled]
- MEBx Debug Message Output** **[Disabled]**  
This option enables or disables the MEBx Debug message output. Configuration options: [Disabled] [Enabled]
- Un-Configure ME** **[Disabled]**  
This option Un-Configures ME without password. Configuration options: [Disabled] [Enabled]
- AMT Wait Timer 0**  
This option sets the timer to wait before sending ASF\_GET\_BOOT\_OPTIONS. Range: 0 – 9999
- Disable ME** **[Disabled]**  
This option sets the ME to soft temporary disabled. Configuration options: [Disabled] [Enabled]
- ASF** **[Enabled]**  
This option enables or disables the Alert Specification Format. Configuration options: [Disabled] [Enabled]
- Activate Remote Assistance Process** **[Disabled]**  
This option triggers the CIRA boot. Configuration options: [Disabled] [Enabled]
- USB Configure** **[Disabled]**  
This option enables or disables the USB configuration function. Configuration options: [Disabled] [Enabled]
- PET Progress** **[Enabled]**  
This option enables or disables the PET events progress. Configuration options: [Disabled] [Enabled]
- WatchDog** **[Disabled]**  
This option enables or disables the Watchdog timer. Configuration options: [Disabled] [Enabled]

## Sub Menu ➤ USB Configuration

USB Configuration	
USB Modul Version	8.10.34
USB Controllers 2 EHCIs, 1 XHCI	
USB Devices: 1 Keyboard, 1 Mouse, 2 Hubs	
Legacy USB Support	[Enabled]
USB3.0 Support	[Enabled]
XHCI Hand-off	[Enabled]
EHCI Hand-off	[Enabled]
XHCI Mode	[Auto]
XHCI Pre-Boot Driver	[Enabled]
Route USB 2.0 pins to which HC?	[Route all Pins to EHCI]
Enable USB 3.0 pins	[Disable all Pins]
USB Ports Per-Port Disable Control	[Disabled]
USB Mass Storage Driver Support	[Enabled]
PORT 60/64 Emulation	[Enabled]
USB Hardware delays and time outs:	
Device power- up delay	[Auto]

### Legacy USB Support

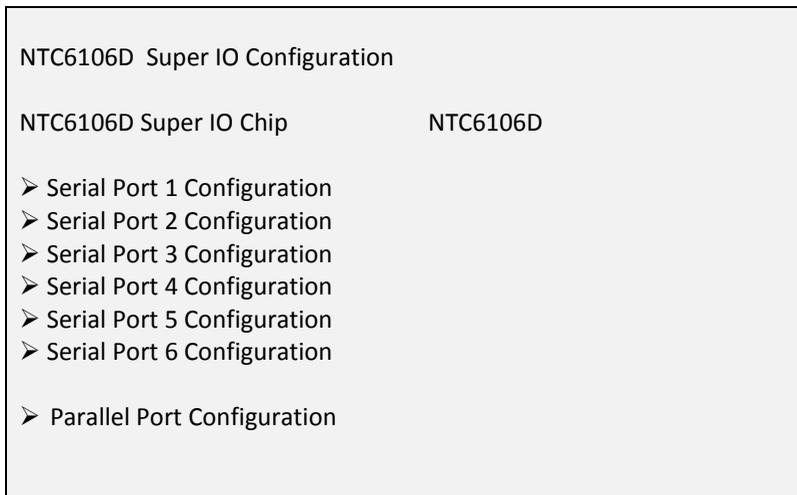
[Enabled]

This option enables the legacy USB support. AUTO option disables legacy support if no USB devices are connected. Disable this option keep USB devices available only for EFI applications.

Configuration options: [Disabled] [Enabled] [Auto]

- USB3.0 Support** **[Enabled]**  
This option enables the USB 3.0 (XHCI) Controller support.  
Configuration options: [Disabled] [Enabled]
- XHCI Hand-off** **[Enabled]**  
Enables support for operating systems without an XHCI hand-off feature.  
Configuration options: [Disabled] [Enabled]
- EHCI Hand-off** **[Enabled]**  
Enables support for operating systems without an EHCI hand-off feature.  
Configuration options: [Disabled] [Enabled]
- XHCI Mode** **[Auto]**  
Mode of Operation of XHCI controller.  
Configuration options: [Smart Auto] [Auto] [Enabled] [Disabled] [Manual]
- USB Ports Per-Port Disable Control** **[Disabled]**  
This option control USB ports disabling. If option is enabled each USB port can be separately disabled.  
Configuration options: [Disabled] [Enabled]
- USB Mass Storage Driver Support** **[Enabled]**  
This option enables or disables the USB Mass storage driver support.  
Configuration options: [Disabled] [Enabled]
- PORT 60/64 Emulation** **[Enabled]**  
This option enables or disables the I/O port 60/64h emulation support.  
Configuration options: [Disabled] [Enabled]
- Device Power-up delay** **[Auto]**  
Maximum time the device will take before it properly reports itself to the host controller. [Auto] uses default values: for a root port it is 100ms, for a Hub port the delay is taken from the Hub descriptor.  
Configuration options: [Auto] [Manual]  
Device Power-up delay in seconds **[5]**  
This time delay is for each USB-Storage Device.

## Sub Menu ➤ NTC6106D Super IO Configuration



The Super IO Configuration for Serial Port 1 – 6 are only an information sub menu which shown their associated properties.

## Sub Menu ➤ NTC6106D Super IO Configuration ➤ Parallel Port Configuration

### Parallel Port [Enabled]

This option enables or disables parallel port (LPT/LPTE).  
Configuration options: [Disabled] [Enabled]

### Change Settings

[Auto]

This option selects several settings for parallel port (LPT/LPTE).  
Configuration options: [Auto] [IO=378h; IRQ=5] [IO=378h;  
IRQ=5,6,7,10,11,12] [IO=278h; IRQ=5,6,7,10,11,12] [IO=3BCh;  
IRQ=5,6,7,10,11,12]

### Device Mode

[STD Printer Mode]

This option selects several options of the printer port mode (LPT/LPTE).  
Configuration options: [STD Printer Mode] [SPP Mode] [EPP-1.9 and SPP  
Mode] [EPP-1.7 and SPP Mode] [ECP Mode] [ECP and EPP-1.9 Mode]  
[ECP and EPP-1.7 Mode]

## Sub Menu ➤ NTC6106D H/W Monitor

PC Health Status	
SYS Thermistor Temp	: +53.5°C/+128°F
PECI Agento Temp	: +89.5°C/+193°F
CPU Diode Temperature	: +88.5°C/+191°F
AUXTIN Temperature	: +34.5°C/+94°F
CPU Fan Speed	: 3543 RPM
PSU Fan Speed	: 4655 RPM
VCORE	: +1.744 V
+5V (VIN0)	: +5.160 V
+12V (VIN1)	: +12.096 V
AVCC	: +3.312 V
VCC3V	: +3.376 V
VSBB	: +3.348 V
VBAT	: +3.056 V

The H/W Monitor is only an information screen which shows all system temperatures, voltages and fan speeds.

## Sub Menu ➤ Intel TXT Information

Chipset	Production Fused
Chipset TXT	Not Supported
CPU TXT	Not Supported
Error Code	None
Class Code	None
Major Code	None
Minor Code	None

**Sub Menu ➤ Serial Port Console Redirection**

COM0 (Disabled) Console Redirection	Port is disabled
COM1 (PCI Bus0, Dev0, Func0) Console Redirection	Port is disabled
Legacy Console Redirection ➤ Legacy Console Redirection Settings	
Serial Port for Out-of-Band Management/ Windows Emergency Management Services (EMS) Console Redirection	[Enabled]
➤ Console Redirection Settings	

**Console Redirection [Enabled]**

This option enables or disables the console redirection.  
Configuration options: [Disabled] [Enabled]

**Sub Menu ➤ Serial Port Console Redirection ➤ Console Redirection Settings**

The settings specify how the host computer will exchange data.  
Both computers should have the same or compatible settings.

Out-of-Band Mgmt	[Com0 (Disabled)]
Terminal Type	[VT-UTF8]
Bits per second	[115200]
Flow Control	[None]
Data Bits	8
Parity	None
Stop Bits	1

**Out-of-Band Mgmt****[Com0 (Disabled)]**

This option enables or disables COM0 or COM1 for serial redirection.

Configuration options: [Com0 (Disabled)] [COM1(PCI Bus0,Dev0,Func0) (Disabled)]

**Terminal Type****[VT-UTF8]**

This option selects a preferred terminal type for Out-of-Band Management.

Configuration options: [VT100] [VT100+I] [VT-UTF8] [ANSI]

**Bits per second****[115200]**

This option selects the serial port transmission speed.

Configuration options: [9600] [19200] [57600] [115200]

**Flow Control****[None]**

This option selects the serial port flow control.

Configuration options: [None] [Hardware RTS/CTS] [Software Xon/Xoff]

**Sub Menu ➤ Network Stack Configuration**

Network Stack	[Disabled]
Ipv4 PXE support	[Enabled]
PXE boot wait time	0
Media detect count	1

**Sub Menu ➤ CMOS**

CMOS Settings/Information	
Bad battery detected:	[False]
First boot detected	[False]
Defaults loaded	[False]
Bad checksum detected	[False]

The CMOS menu is only an information screen which shows some specific CMOS information.

**Sub Menu > Intel(R) Ethernet Network Connection**

> NIC Configuration	
Blink LED (range 0-15 seconds)	0
UEFI Driver	Intel(R) 1GbE DEV 5.1.00
Adapter PBA	FFFFFF-OFF
Device Name	Intel® Ethernet Connec
Chip Type	Intel PCH LPT
PCI Device ID	153A
PCI Address	0:25:0
Link Status	[Disconnected]
Factory MAC Address	AC:DC:FA:DE:BE:EF

**Sub Menu > Intel(R) Ethernet Network Connection > NIC Configuration**

**Link Speed**

**[AutoNegotiated]**

This option selects a preferred link speed and duplex for current LAN port.  
Configuration options: [AutoNeg] [10 Mbps Half] [10 Mbps Full] [100 Mbps Half] [100 Mbps Full].

**Wake On LAN**

**[Enabled]**

This allows enabling or disabling power up the BEETLE when the LAN controller receives a call while the BEETLE is in Soft-Off or Hibernate mode.  
Configuration options: [Disabled] [Enabled].

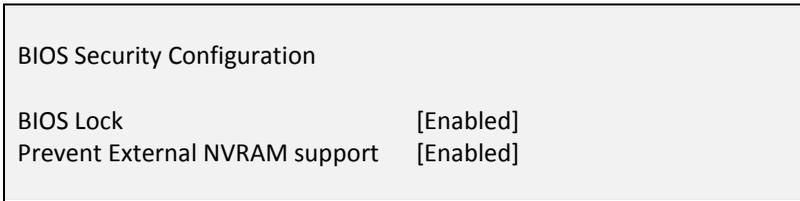
## Chipset Menu



### Sub Menu ➤ PCH-IO Configuration



### Sub Menu ➤ PCH-IO Conf. ➤ BIOS Security Configuration



#### **BIOS Lock** [Enabled]

This option enables or disables the BIOS lock enable (BLE) bit.  
Configuration options: [Disabled] [Enabled]

#### **BIOS Interface Lock** [Enabled]

This option handles the NVRAM access. For using a NVRAM module set this option to [Disabled].  
Configuration options: [Disabled] [Enabled]

## Sub Menu ➤ System Agent (SA) Configuration

System Agent Bridge Name	Haswell
System Agent RC Version	1.9.0.0
Vt-d Capability	Supported
➤ Graphics Configuration	

## Sub Menu ➤ System Agent (SA) Configuration ➤ Graphics Configuration

Graphics Configuration	
IGFX VBIOS Version	1039
IGFX Frequency	700 MHz
Graphics Turbo IMON Current	31
Primary Display	[Auto]
Primary PEG	[Auto]
Primary PCIE	[Auto]
Internal Graphics	[Auto]
Aperture Size	[256MB]
DVMT Pre-Allocated	[32MB]
DVMT Total Gfx Mem	[256MB]
Gfx Low Power Mode	[Enabled]
Internal Graphics Port Order	[VGA>Disp.1>Disp.2]

### Graphics Turbo IMON Current **[Enabled]**

This option sets the Graphics Turbo IMON current value.  
Configuration options: 14-31

### Primary Display **[Auto]**

This option selects which graphics device IGFX, PEG, PCI should be the primary display.  
Configuration options: [Auto] [IGFX] [PEG] [PCIE]

**Primary PEG** **[Auto]**  
This option selects which graphics device PEG11, PEG12 should be the primary PEG.  
Configuration options: [Auto] [PEG11] [PEG12]

**Primary PCIE** **[Auto]**  
This option selects which graphics device PCIE1-7 should be the primary PCI. Configuration options: [Auto] [PCIE1] [PCIE2] [PCIE3] [PCIE4] [PCIE5] [PCIE6] [PCIE7]

**Internal Graphics** **[Auto]**  
This option keeps the IGD enabled based on the setup option.  
Configuration options: [Auto] [Disabled] [Enabled]

**Aperture Size** **[256MB]**  
This option sets the aperture size of the graphics device.  
Configuration options: [128MB] [256MB] [512MB]

**DVMT Pre-Allocated** **[32MB]**  
This option selects DVMT 5.0 pre-allocated graphics memory size used by the internal graphics device.  
Configuration options: [32MB] - [1024MB]

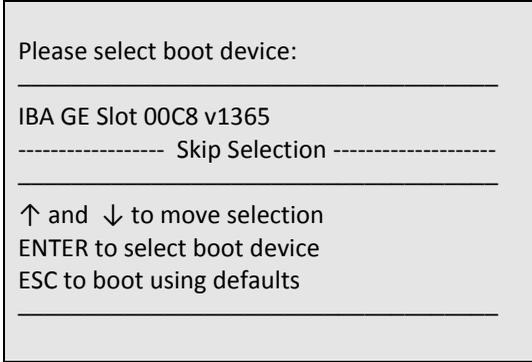
**DVMT Total Gfx Mem** **[256MB]**  
This option selects DVMT 5.0 total graphics memory size used by the internal graphics device.  
Configuration options: [128MB] [256MB] [MAX]

**Gfx Low Power Mode** **[Enabled]**  
This option is application for SFF only  
Configuration options: [Disabled] [Enabled]

**Internal Graphics Port Order** **[VGA>Disp.1>Disp.2]**  
This option selects which device may be used as primary display first  
Configuration options: [VGA>Disp.1>Disp.2] [Disp.1>Disp.2>VGA] [VGA>Disp.2>Disp.1] [Disp.2>Disp.1>VGA] [Disp.1>VGA>Disp.2] [Disp.2>VGA>Disp.1]

## Boot Menu

The Boot Menu enables you to set the order of bootable devices to a regular base. Pressing the function key <F10> while POST is running will change the boot order only once. You will see a Pop-Up window listing all devices the system is able to boot from. Select the boot device with keys <Up> and <Down>. Press <Enter> key to start the selected device booting.



<b>Boot Configuration</b>	
Setup Prompt Timeout	5
Bootup NumLock State	[On]
Quiet Boot	[Disabled]
Fast Boot	[Disabled]
Boot mode select	[Legacy]
Fixed Boot Order Priorities	
Boot Option #1	[USB Floppy]
Boot Option #2	[USB Key]
Boot Option #3	[USB Hard Disk]
Boot Option #4	[USB CD/DVD]
Boot Option #5	[CD/DVD]
Boot Option #6	[Hard Disk]
Boot Option #7	[Network]
➤ CSM parameters	

**Bootup NumLock State** **[On]**

Select the keyboard Numlock State  
Configuration options: [On] [Off]

**Quiet Boot** **[Disabled]**

This option disables the POST messages while booting.  
Configuration options: [Disabled] [Enabled]

**Fast Boot** **[Disabled]**

Enables or disables boot with initialization of minimal set of devices required to launch activate boot option. Has no effect for BBS boot options  
Configuration options: [Disabled] [Enabled]

**Boot mode select** **[LEGACY]**

This option selects the boot mode.  
If you choose UEFI the system will only boot from UEFI devices. All other devices will not be shown.  
Configuration options: [LEGACY] [UEFI]

**Fixed Boot Order Priorities ‘#n’ Boot Device**

These menu entries are used to specify the boot sequence from the available devices. Every entry (from #1 till #7) specifies a boot group. Each boot device found while POST is running will be sorted in one of a BBS group. Enter a BBS group to swap the boot order of the BBS device.

## Security Menu

<b>Password Description</b>	
If only the Administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup.	
The password length must be	
In the following range	
Minimum length	3
Maximum length	20
Administrator Password	
Intrusion detection	[Disabled]
Case Status	[Closed]
➤ Secure Boot menu	

### Administrator Password

This field allows you to set the password. Highlight the field and press <Enter>. Type a password and press <Enter>, you can type **3 to 20** alphanumeric characters. Symbols and other characters are ignored. To confirm the password, type the password again and press <Enter>. This password allows full access to the UEFI BIOS Setup menu. To clear the password, highlight this field and press <Enter>. Enter your current password. Then you will be asked to enter the new password. Press <Enter> and the password will be deleted.

### Intrusion Detection

**[Disabled]**

If the system cover is removed and the Intrusion Detection is [Enabled], the system stops during the next reboot or power up process and display a warning message. After this warning the boot process stops and the user has to enter the UEFI BIOS setup which resets the open case detection automatically. Additionally is a viewing point of the case open switch

below the enable/disable entry point placed. This message will signalize the actual case open status directly.

Configuration Options: [Disabled] [Enabled]

### Sub Menu ➤ Secure Boot menu

System Mode	Setup
Secure Boot	Not Active
Secure Boot	[Enabled]
Secure Boot Mode	[Standard]

#### Secure Boot

**[Enabled]**

This option can be enabled if:

1. System running in User mode with enrolled Platform Key
2. CSM function is disabled

Configuration options: [Disabled] [Enabled]

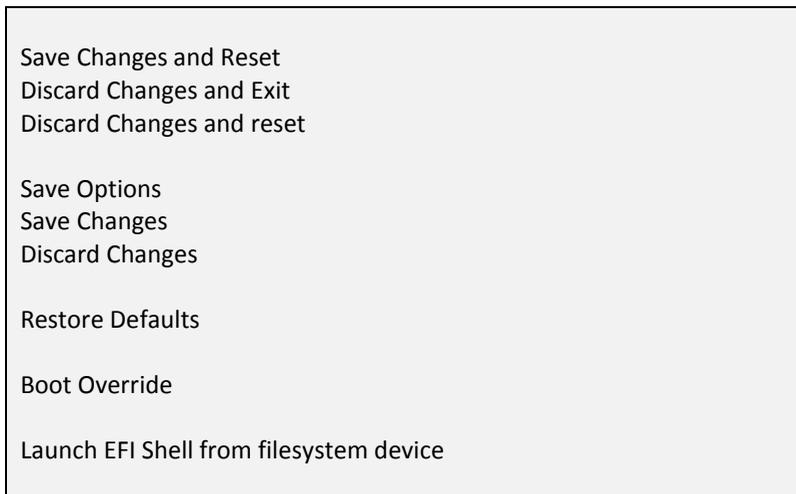
#### Secure Boot Mode

**[Standard]**

This is the secure mode selector. The 'Custom' mode enables user to change the Image Execution policy and manage Secure Boot Keys

Configuration options: [Standard] [Custom]

## Save & Exit Menu



Once made all selections from the various menus in the Setup program, save changes should execute and leave Setup. Select Exit from the menu bar to display the following menu.

### **Discard Changes and Exit**

This option should only be used if the changes made in Setup should not save. If made some changes to fields other than system date, system time, and password, the system will ask for confirmation before exiting.

### **Save Changes and Reset**

Once finished changing setup values, this option from the Exit menu ensure that values are saved to the NVRAM. The NVRAM is sustained by an onboard backup battery and stays on even when the BEETLE is turned off. Once this option is selected, a confirmation is asked. Select [OK] to save changes and reset the system.

### **Discard Changes and Reset**

This option should only be used if the changes made in Setup should not save. If made some changes to fields other than system date, system time, and password, the system will ask for confirmation before exiting and reset the system.

## Restore Defaults

This option loads the default values for each of the values on the Setup menu. When this option is selected or if <F3> is pressed, a confirmation is requested. Select [Ok] to load default values. Now select Exit Saving to save the default values or make other changes before saving the values to the non-volatile RAM.

## Boot Override

With this option choose a boot device that is listed below this menu entry. Every entry specifies a boot device that enumerate during POST.

## Launch EFI Shell from File System Device

Attempts to launch EFI shell application from one of the available file system devices.

## Test Points Codes

At the beginning of each POST routine, the UEFI BIOS outputs the test point error code to I/O port address 80h. Use this code during trouble shooting to establish where the system failed and what routine has been performed.

## Checkpoint Ranges

Status Code Range	Description
0x01 – 0x0B	SEC execution
0x0C – 0x0F	SEC errors
0x10 – 0x2F	PEI execution up to and including memory detection
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0x8F	DXE execution up to BDS
0x90 – 0xCF	BDS execution
0xD0 – 0xDF	DXE errors
0xE0 – 0xE8	S3 Resume (PEI)
0xE9 – 0xEF	S3 Resume errors (PEI)
0xF0 – 0xF8	Recovery (PEI)
0xF9 – 0xFF	Recovery errors (PEI)

## SEC Phase

Status Code	Description
0x00	Not used
<b>Progress Codes</b>	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization
<b>SEC Error Codes</b>	
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not loaded

## PEI Phase

Status Code	Description
<b>Progress Codes</b>	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)

0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D - 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)

0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
<b>PEI Error Codes</b>	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C-0x5F	Reserved for future AMI error codes
<b>S3 Resume Progress Codes</b>	
0xE0	S3 Resume is started (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4-0xE7	Reserved for future AMI progress codes
<b>S3 Resume Error Codes</b>	
0xE8	S3 Resume Failed
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC-0xEF	Reserved for future AMI error codes
<b>Recovery Progress Codes</b>	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)

0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loaded
0xF5-0xF7	Reserved for future AMI progress codes
<b>Recovery Error Codes</b>	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AMI error codes

## PEI Beep Codes

# of Beeps	Description
1	Memory not Installed
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)
2	Recovery started
3	DXE IPL was not found
3	DXE Core Firmware Volume was not found
4	Recovery failed
4	S3 Resume failed
7	Reset PPI is not available

## DXE Phase

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started

0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect

0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8 – 0xBF	Reserved for future AMI codes
0xC0 – 0xCF	OEM BDS initialization codes
<b>DXE Error Codes</b>	
0xD0	CPU initialization error
0xD1	North Bridge initialization error

0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)

0xDB	Flash update is failed
0xDC	Reset protocol is not available

## **DXE Beep Codes**

# of Beeps	Description
1	Invalid password
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
6	Flash update is failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met

# Abbreviations

<b>ADM</b>	AMI Display Manager
<b>ACPI</b>	Advanced Configuration and Power Interface
<b>AGTL+</b>	Assisted Gunning Transceiver Logic
<b>APC</b>	Advanced Power Control
<b>APIC</b>	Advanced Peripheral Interrupt Controller
<b>APM</b>	Advanced Power Management
<b>AT</b>	Advanced Technology
<b>ATA</b>	AT Attachment
<b>BAT</b>	Basic Access Test
<b>BBS</b>	BIOS Boot Specification
<b>BDA</b>	BIOS Data Area
<b>BGA</b>	Ball Grid Array
<b>BIOS</b>	Basic Input and Output System
<b>CMOS</b>	Complementary Metal Oxide Semiconductor
<b>CPLD</b>	Complex Programmable Logic Device
<b>CPU</b>	Central Processing Unit
<b>CRT</b>	Cathode-ray Tube
<b>DIM</b>	Device Initialization Manager
<b>DIMM</b>	Dual Inline Memory Module
<b>DMA</b>	Direct Memory Access
<b>DMI</b>	Desktop Management Interface
<b>DVMT</b>	Dynamic Video Memory Technology
<b>DVI</b>	Digital Video Interface
<b>EBDA</b>	Extended BIOS Data Area
<b>ECP</b>	Extended Capabilities Port
<b>EEPROM</b>	Electrical Erasable Read Only Memory
<b>EFI</b>	Extensible Firmware Interface
<b>E-IDE</b>	Enhanced Integrated Drive Electronics
<b>EMS</b>	Expanded Memory System
<b>ESCD</b>	Extended System Configuration Data
<b>EPP</b>	Enhanced Parallel Port
<b>FSB</b>	Front Side Bus

<b>GPNV</b>	General Purpose Non-Volatile (RAM)
<b>GTL</b>	Gunning Transceiver Logic
<b>HW</b>	Hardware
<b>IDE</b>	Integrated Drive Electronics
<b>IGD</b>	Internal Graphic Device
<b>IPL</b>	Initial Program Load (Device)
<b>LAN</b>	Local Area Network
<b>LBA</b>	Logical Block Addressing
<b>LCD</b>	Liquid Crystal Display
<b>MAC</b>	Media Access Control
<b>MTRR</b>	Memory Type Range Register
<b>MP</b>	Multiple Processors
<b>NA</b>	Power failure
<b>NVRAM</b>	Non-volatile Random Access Memory
<b>P-ATA</b>	Parallel AT Attachment (old version of hard disk interface)
<b>POS</b>	Point of Sales
<b>PCI</b>	Peripheral Component Interconnect
<b>PnP</b>	Plug and Play
<b>POST</b>	Power On Self Test
<b>RAM</b>	Random Accessible Memory
<b>RI</b>	Ring Indicator
<b>ROM</b>	Read Only Memory
<b>RS</b>	Retail Systems
<b>SATA</b>	Serial AT Attachment (new version of hard disk interface)
<b>SLP</b>	System Locked Pre-Installation
<b>SMI</b>	System Management Interrupt
<b>SMM</b>	System Management Mode
<b>SMRAM</b>	System Management RAM
<b>SPGA</b>	Staggered Pin Grid Array
<b>TFT</b>	Thin-film transistor

<b>TPM</b>	Trusted Platform Module
<b>UEFI</b>	Unified Extensible Firmware Interface
<b>UPS</b>	Uninterruptible Power Supply
<b>USB</b>	Universal Serial Bus
<b>UUID</b>	Universal Unique Identifier
<b>VGA</b>	Video Graphics Array
<b>WOL</b>	Wake On LAN
<b>WOM</b>	Wake On Modem



Diebold Nixdorf Systems GmbH  
D-33094 Paderborn

Order No.: **01750266921B**