

集特海光通用服务器BIOS配置说明书

# 用户使用手册(标准版)

# GME-5002-01

版本: Ver1.0

北京集特智能科技有限公司

www.graest.com

1 BIOS	; 概述	1
1.1	1 基本功能	1
2 BIOS	配置界面介绍	2
2.1	1 概述	2
	2.1.1 进入百敖 UEFI BIOS 的配置界面	2
	2.1.2 页面布局	2
2.2	2 主页界面功能描述	3
	2.2.1 处理器信息	4
	2.2.2 内存信息	5
	2.2.3 系统日期和时间	7
	2.2.4 系统概述	7
	2.2.5 PSP 固件版本	8
	2.2.6 选择语言	9
2.3	<b>3</b> 设备页面功能描述	10
	2.3.1 PCIE 配置	11
	2.3.2 显示配置	12
	2.3.3 SATA 配置	13
	2.3.4 SATA 设备信息	14
	2.3.5 NVME 设备	15
	2.3.6 USB 配置	16
	2.3.7 PCI 设备信息	17
2.4	4 高级界面功能描述	18
	2.4.1 串口重定向	19
	2.4.2 服务管理	21
	2.4.3 RTC 唤醒	23
	2.4.4 海光设置	24
	2.4.5 UEFI HII 配置	25
2.5	5 安全界面功能描述	26
	2.5.1 设置管理员/用户密码	27
	2.5.2 TCG2 配置	29
	2.5.3 硬盘密码	29
	2.5.4 TCM 配置	31
	2.5.5 安全启动	32
2.6	δ 启动界面功能描述	34
2.7	7 退出界面功能描述	35

目 录

# 1 BIOS 概述

BIOS(Basic Input Output System) 基本输入输出系统,是加载在计算机主板芯片上最 基本的程序代码。它保存着计算机最重要的基本输入输出的程序、开机后自检程序和系统 自启动程序。其主要功能是为计算机提供最底层的、最直接的硬件设置和控制,寻找启动 设备,启动系统或其他预引导环境等。

百敖 UEFI 固件是遵循 UEFI 2.7 版本的规范要求的标准固件产品。其适用于同泰怡海 光 T2DMHG 和 T2DEHG 项目,用于初始化平台的硬件和加载并引导操作系统。

本文档适用于百敖 UEFI BIOS 固件,简单描述了 BIOS 配置界面中选项的功能及相应的设置方法。

主页设备高级安	全启动退出	百熬ByoCore软件U1.8	
		百敖软件 百敖CRB2.0	帮助信息
发布版本 固件生成时间		00.07 08/15/2022 13:25	处理器信息
主板信息		теля T2DMHG	
<ul> <li>▶ 处理器信息</li> <li>▶ 内存信息</li> <li>▶ 系统日期和时间</li> <li>▶ 系统概述</li> <li>▶ PSP固件版本</li> </ul>			
用户登录类型 选择语言		管理员 <中文>	
P1 帮助 Esc 退出	11 选项条目 ↔ 选择菜单	-/+ 更改设置 Enter 选择子菜单	P9 默认值 F10 保存并退出
	Сор	uright (C) 2006-2022,百敖软件有限公司	

#### 图 1-1 BIOS 主界面

## 1.1 基本功能

- ✔ 符合 UEFI 2.7/PI 2.1.0.2 规范
- ✔ 支持串口重定向
- ✓ 支持 USB 键盘、鼠标
- ✓ 支持通过 USB 设备安装、启动操作系统
- ✓ 支持 PXE 启动
- ✔ 支持配置界面中、英文显示
- ✓ 具备 UEFI BIOS 的其他基本功能

# **2** BIOS 配置界面介绍

# 2.1 概述

配置界面是百敖 UEFI BIOS 提供的用于显示、设置、修改 BIOS 选项的环境,该界面 支持 USB 键盘以及串口重定向操作,能够提供多种语言显示(默认支持中文)。 本文描述了配置界面的使用方法。

## 2.1.1 进入百敖 UEFI BIOS 的配置界面

在按下平台的 Power Button 按钮以后, BIOS 开始执行平台硬件初始化, 通过串口接 收工具,当看到串口输出 "Press Del to enter SETUP, and Press F11 to enter Boot Menu, and Press F12 to enter PXE boot."信息后,按下 Delete 键,即可进入百敖 UEFI BIOS 的配置界面。

## 2.1.2 页面布局

页面说明区域			
页面说明区域	选项帮助信息说 明区域		
操作帮助说明区域			
页面说明区:显示各个主页面的标题,如:主页、高级、安	全等		

BIOS 配置界面的每个页面每个页面均按如图 2-1 所示排版: 图 2-1 配置界面页面布局

- ▶ **选项配置区:**提供相关选项的显示、配置等功能
- ▶ 选项说明区:提供选项的帮助说明信息
- 操作说明区:提供如何在配置界面中进行修改、保存操作的说明  $\triangleright$

## 2.2 主页界面功能描述

当在 BIOS 启动过程中按下"Delete"键后,BIOS 默认显示此页面。

主页页面主要用来显示平台信息,包括固件厂商、固件版本、发布版本、固件生成时间、BMC 状态、主板信息、处理器信息、内存信息、系统日期和时间、系统概述、PSP 固件版本、用户登录类型及选择语言,如图 2-2 所示:

主页 设备 高级 安全 启动 退出	百敗ByoCore软件U1.0	
固件厂商 固件版本	百敖软件 百赦CRB2 A	帮助信息
发布版本 固件生成时间	00.07 08/15/2022 13:25	处理器信息
BMC状态 主板信息	正常 T2DMHG	
<ul> <li>▶ 处理器信息</li> <li>▶ 内存信息</li> <li>▶ 系统日期和时间</li> <li>▶ 系统概述</li> <li>▶ PSP圖件版本</li> </ul>		
用户登录类型 选择语言	管理员 <中文>	
21 帮助 11 选项条目 16 退出 ———————————————————————————————————	/+ 更改设置 Poter 洗择子菜单	19 默认值 F10 保存并退出

图 2-2 主页页面

- ▶ 固件厂商: 百敖软件
- ▶ **固件版本:** 百敖 CRB2.0
- ▶ 发布版本: 00.07 (依据实际版本号显示)
- ▶ 固件生成时间:08/15/2022 13:25 (依据主板固件实际生成时间显示)
- ▶ BMC 状态:正常(依据主板 BMC 实际状态显示)
- ▶ 主板信息: T2DMHG(或 T2DEHG)
- ▶ 处理器信息: CPU 数量、CPU 厂商、CPU 型号、CPU 核数、CPU 线程数、CPU 频率、CPU 内存通道数、L1 缓存大小、L2 缓存大小、L3 缓存大小、CPU 热设计功耗、CPU 序列号
- 内存信息:内存总容量、内存当前频率、内存插槽类型、内存插槽总数、内存空插槽总数、内存总数量及内存在位状态等
- **系统日期和时间:**显示和修改系统日期和时间,日期和时间的修改方法请参考右侧的 帮助信息
- ▶ 系统概述: 主机商标标识、主机编号、资产管理名称、系统 UUID、UEFI 版本号、 SMBIOS 版本号、PI 版本、CSM 发布时间
- ▶ 用户登录类型:管理员或者普通用户
- ▶ 选择语言:中文/English

## 2.2.1 处理器信息

若光标的焦点在"处理器信息"时,按下"Enter"键,则会进入处理器信息子页面, 如图 2-3 所示:

百封UgeCore著件U1.0			
处理	<b>王器信息</b>	帮助信息	
处理器信息			
处理器1 处理器类型 处理器加 处理器频率 处理器热设计功耗 处理器电压 一级数据缓存大小(每座) 一级指令缓存大小(每座) 二级缓存大小(每座) 三级缓存大小(每座) 三级缓存大小(每座) 三级缓存大小(每座) 处理器核心数量 处理器微码补丁版本	Hygon C86 7385 32-core Processor 0x900F22 (Family 24, Model 2, Stepping 2) 2000 MHz 190 W 1.0V 1024 KB / 8-Way 2048 KB / 4-Way 16384 KB / 8-Way 64 MB / 64-Way 32 Core(s) / 64 Thread(s) 0x80901047		
处理器2 处理器10 处理器频率 处理器热设计功耗 处理器电压 一级数据缓存大小(每座) 二级缓存大小(每座) 二级缓存大小(每座) 三级缓存大小(每座) 处理器微码补丁版本	Hygon CB6 7305 32-core Processor 0x900F22 (Family 24, Model 2, Stepping 2) 2000 MHz 190 W 1.0U 1024 KB / 8-Way 2048 KB / 8-Way 16384 KB / 8-Way 64 MB / 64-Way 32 Core(s) / 64 Thread(s) 0x80901047		
11 - 売び条目 Bac 退出 → 选择菜单	····· 更改设置 Enter 选择子菜单 Copyright (C) 2906-2022,百敖软件有限公司	户) 默认值 F10 保存并退出	

#### 图 2-3 处理器信息页面

- ▶ 处理器1
- ▶ 处理器类型: Hygon C86 7385 32-core Processor
- ▶ 处理器 ID: 0x900F22 (Family 24, Model 3. Stepping 2)
- ▶ 处理器频率: 2000 MHZ
- ▶ 处理器热设计功耗: 190 W
- ▶ 处理器电压: 1.0V
- ➤ 一级数据缓存大小(每座): 1024 KB / 8-Way
- ➤ 一级指令缓存大小(每座): 2048 KB / 4-Way
- ▶ 二级缓存大小(每座): 16384 KB / 8-Way
- ➢ 三级缓存大小(每座): 64 MB / 64-Way
- ▶ 处理器核心数量: 32 Core(s) / 64 Thread(s)
- ▶ 处理器微码补丁版本: 0x80901047
- ▶ 处理器 2
- ▶ 处理器类型: Hygon C86 7385 32-core Processor
- > 处理器 ID: 0x900F22 (Family 24, Model 3. Stepping 2)
- ▶ 处理器频率: 2000 MHZ
- ▶ 处理器热设计功耗: 190 W
- ▶ 处理器电压: 1.0∨
- ➤ 一级数据缓存大小(每座): 1024 KB / 8-Way
- ➤ 一级指令缓存大小(每座): 2048 KB / 4-Way

- ▶ 二级缓存大小(每座): 16384 KB / 8-Way
- ▶ 三级缓存大小 (每座): 64 MB / 64-Way
- > 处理器核心数量: 32 Core(s) / 64 Thread(s)
- ▶ 处理器微码补丁版本: 0x80901047

## 2.2.2 内存信息

若光标的焦点在"内存信息"时,按下"Enter"键,则会进入内存信息子页面,如图 2-4 所示:

百赦山pCmre软件01.0				
	内存信息		帮助信息	
内存总容量 内存速度		16 GB 2133 MT/s	CPU 1	
▶ CPU 1 ▶ CPU 2				
PI 帮助 Esc 退出	11 选项条目 ➡ 选择菜单	─/*   史改设置 Diter 选择子菜单	F5 默认值 F10 保存并退出	
Copyright (C) 2006-2022, 百敖软件有限公司				

图 2-1 内存信息页面

图 2-5 CPU 1 页面

白水山和Grant (特別) 「主页」				
	CPU 1		帮助信息	
内存插槽 62 内存插槽 61 内存插槽 82 内存插槽 81		未安装 未安装 未安装 厂商:Samsung,部件号: <b>H39362K40BB0-CPB</b> , 容量:166B,1Rx4,类型:RDIMM,ECC:Y, 序列号:3342SFFB		
内存存插槽 C2 内存存插槽 D2 内存存插槽 D1 内存存插槽 E2 内存存插槽 F1 内存存插槽 F1 内存存插槽 61 内存插插槽 H1		序列号:33425FEB 未安装 未安装装 未安装装 未安装装 未安装装 未安装装 未安装装 未安装装		
11 帮助	11 选项条目	-/* 更改设置	19 默认值	
Esc 退出	➡ 远择采早	inter 选择于桌里 umight (C) 2005_2022	F18 保仔开退出	
Lopyright (L) 2006-2022, 日默软件有限公司				

图 2-6 CPU 2 页面

百族lgoCore软件U1.0			
	CPU 2		帮助信息
内内存存存存存存存存存存存存存存存存存存存存存存存存存存存存存存存存存存存	未安装装 未安安装装 未安安装装 未来来未未来, 未来安安安安安安安安安安安安安安安安安安安安安安安安安安安安安		
P1 帮助 Bin 退出	11 选项条目 -/+ → 选择菜单 5mt		
	Copyr ight (C) 2006-1	2022,百敖软件有限公司	

▶ 内存总容量:根据当前实际内存总容量显示

▶ 内存速度:根据当前内存速度显示

- ▶ CPU 1:显示各内存插槽状态,若无内存条,显示未安装;若有内存条,则显示其信息
- ▶ CPU 2: 显示各内存插槽状态,若无内存条,显示未安装;若有内存条,则显示其信息

## 2.2.3 系统日期和时间

若光标的焦点在"系统日期和时间"时,按下"Enter"键,则会进入系统日期和时间 子页面,如图 2-7 所示:

系统日期和时间			帮助信息
系统日期(月/日/年) 系统时间(时:分:秒)	[04/01/2021] [06:08:48]		设定日期。 使用Tab键可以在日期区域 切换。系统日期有效范围: 年:2021 - 2099 月:1 - 12 日:1 - 31
□ 帮助   1 Pac 退出	选项条目 -/+ 选择菜单 Pite	更改设置 - 选择子菜单	
	Copyr ight (C) 2006-20	22,百敖软件有限公司	

图 2-7 系统日期和时间页面

- 系统日期(月/日/年):设定日期,使用 Tab 键可以在日期区域切换。可支持从 2021 至 2099 年之间切换
- ▶ 系统时间(时:分:秒):设定时间,使用 Tab 键可以在时间区域切换

## 2.2.4 系统概述

若光标的焦点在"系统概述"时,按下"Enter"键,则会进入系统概述子页面,如图 2-8 所示:

#### 图 2-8 系统概述页面

百放和poCpre软件01.0			
系统概述		帮助信息	
主机商标标识 主机编号 资产管理名称 系统 <b>UUID</b>		Hygon A7199A69-E522-46BF-BE96-3F49BC97F755	
UEFI版本号 SMBIOS版本 Agesa PI版本 CSM发布时间		UEFI 2.70; PI 1.70 3.3 HygonPI 2.1.0.2 08/10/2022	
Fi 希明 Esc 退出	□ 远坝余日 → 选择菜单	・/* 更改成置 Enter 选择子菜单	PD 默认值 F10 保存并退出
	Сор	yright (C) 2006-2022,白默软件有限公司	

- ▶ 主机商标标识: Hygon
- ▶ 主机编号:显示为空表示未写入主机编号
- ▷ 资产管理名称: 显示为空表示未写入资产管理名称
- ▶ 系统 UUID: 系统唯一标识符
- ▶ UEFI版本号: UEFI 2.70; PI 1.70
- ➢ SMBIOS 版本号: 3.3
- ▶ Agesa PI 版本: HygonPI 2.1.0.2
- ▶ CSM 发布时间: 08/10/2022

## 2.2.5 PSP 固件版本

若光标的焦点在 "PSP 固件版本"时,按下 "Enter"键,则会进入 PSP 固件版本子 页面,如图 2-9 所示:

#### 图 2-9 PSP 固件版本页面

百族與oCpre软件01.0			
	PSP固件版本	帮助信息	
PSP启动加载器版本 SMU固件版本 ABL固件版本 APCB固件版本 APOB固件版本 APDB固件版本	1.3.33.0 1.6.95 1.3.47.0 0.37 0.12 0.1		
	条目 -/* 更改设置 蓝单 -/* 选择子蓝单		
	Copyright (C) 2006-2022,百敖软件有[	限公司	

- PSP 启动加载器版本: 1.3.33.0
   SMU 固件版本: 1.6.95
- ➤ ABL 固件版本: 1.3.47.0
- ➤ APCB 固件版本: 0.37
- ➢ APOB 固件版本: 0.12
- ➢ APPB 固件版本: 0.1

## 2.2.6 选择语言

该根据需要选择合适的语言,默认显示中文。如图 2-10 所示: 图 2-10 选择语言信息页面



# 2.3 设备页面功能描述

该页面显示 PCIE 配置、显示配置、SATA 配置、SATA 设备信息、NVME 设备、 USB 配置、PCI 设备信息,如图 2-11 所示:

图 2-11 设备页面

主页 <mark>设备</mark> 高级 安全 启动 退出	百衆UgaCore软件01.8	
netr和罢		帮助信息
<ul> <li>PCITAE首</li> <li>显示配置</li> <li>SATA设备信息</li> <li>NUFE设备</li> <li>USD配置</li> <li>PCT设备信息</li> </ul>		PCIE配置
	-/* 更改设置	
196 巡山 一 四洋来早	Comuright (C) 2006-2022,百敖软件有限公司	F18 体行开巡山

- ▶ PCIE 配置:此选项用以设置 PCIE 相关配置
- ▶ 显示配置:此选项用以设置显示相关配置
- > SATA 配置:此选项用以设置和显示 SATA 相关配置
- ▶ SATA 设备信息:此选项用以显示 SATA 设备信息
- ▶ NVME 设备:此选项用以显示 NVME 设备信息
- ▶ USB 配置:此选项用以设置和显示 USB 相关配置
- ▶ PCI 设备信息:此选项用以显示 PCI 设备信息

## 2.3.1 PCIE 配置

若光标的焦点在 "PCIE 配置"时, 按下 "Enter"键, 则会进入 PCIE 配置子页面, 如图 2-12 所示:

#### 图 2-12 PCIE 配置页面

设备	百敖ByaCore软件U1.0	
PCIE	記置	帮助信息
PCTE# PCTE#英醒 SM PORT0 M.2 SLOT0 (CPU1) OCP CPU1 SLIM0_1 (J51 X4) CPU1 SLIM0_2 (J51 X4) CPU1 LANE 80°95 CPU1 LANE 112°127 M.2 SLOT1 (CPU2) CPU2 SLIM1 (J53 X8) RISER2_3 (X8) RISER2_2 (X8) RISER2_2 (X8) RISER2_2 (X8) PCTE状态列表 M.2 SLOT0 (CPU1) Gen3/Gen4 2X/2X NUMe (ID:2 OCP Gen2/Gen4 4X/BX Ethernet controller (I RISER3_1 (X8) Gen1/Gen4 1X/BX Ethernet controller (I)	記重 (打开) (TT)	种助信息.         开启或关闭PCIE唤醒
P1 帮助	/+ 更改设置 <u>Citter</u> 选择子菜单	▶️ 默认值 ₽10 保存并退出

▶ PCIE 唤醒:打开或关闭 PCIE 唤醒

以下选项根据主板上实际 PCIE 接口显示

- ▶ SM PORTO: 打开或关闭 SM PORTO
- > M.2 SLOT0(CPU1): 打开或关闭 M.2 SLOT0(CPU1)
- ▶ OCP: 打开或关闭 OCP
- ▶ CPU1\_SLIM0\_1(J51 X4): 打开或关闭 CPU1\_SLIM0\_1(J51 X4)
- ▶ CPU1\_SLIM0\_2(J51 X4): 打开或关闭 CPU1\_SLIM0\_2(J51 X4)
- > CPU1 LANE 80~95:打开或关闭 CPU1 LANE 80~95
- > CPU1 LANE 112~127:打开或关闭 CPU1 LANE 112~127
- ▶ M.2 SLOT1(CPU2): 打开或关闭 M.2 SLOT1(CPU2)
- > CPU2 SLIM1(J53 X8): 打开或关闭 CPU2 SLIM1(J53 X8)
- > RISER2\_3(X8): 打开或关闭 RISER2\_3(X8)
- > RISER2\_2(X8): 打开或关闭 RISER2\_2(X8)
- ▶ RISER2\_1(X8): 打开或关闭 RISER2\_1(X8)
- ▶ RISER3\_1(X8): 打开或关闭 RISER3\_1(X8)
- > RISER3\_2(X8): 打开或关闭 RISER3\_2(X8)
- ▶ PCIE 状态列表:显示当前 PCIE 接口所接设备信息

### 2.3.2 显示配置

若光标焦点在"显示配置"时,当按下"Enter"键,则会进入该子页面,如图 2-13 所示:

#### 图 2-13 显示配置页面

设备		百款ByoCore软件01.0	
	显示配置		帮助信息
优先显示控制器 板载显卡 外插显卡		《所有显卡》 ASPEED BMC 2500 未安装	选择优先使用哪个设备做视频输出
11 帮助 11 Ese 退出 44	选项条目 选择菜单	→··· 更改设置 Satar 选择子菜单	755 默认值 2166 保存并退出
	Сору	right(C)2006-2022,百敖软件有限公司	

- ▶ 优先显示控制器:选择优先显示的显卡,默认为所有显卡
- ▶ 板载显卡: ASPEED BMC 2500
- ▶ 外插显卡:根据实际外插显卡型号显示

## 2.3.3 SATA 配置

若光标焦点在"SATA 配置"时,当按下"Enter"键,则会进入该子页面,如图 2-14 所示:

#### 图 2-14 SATA 配置页面

·····································	百款BynCore软件01.0	
SATARE	ł	帮助信息
SATA控制器1(REAR SATA PORTO CPU1) SATA Port1 SATA Port2 SATA Port3 SATA Port4 SATA控制器2(SATA PORTO CPU1 & SATA PORT1 CPU1) SATA Port1 SATA Port1 SATA Port2 SATA Port3 SATA Port5 SATA Port5 SATA Port5 SATA Port5 SATA Port6 SATA Port8 SATAPort8 SATAPort1 SATA Port1 SATA Port1 SATA Port1 SATA Port2 SATA Port3 SATA Port3 SATA Port4		开启或关闭SaTa控制器
P1 帮助 11 选项条目 DSC 退出 → 选择菜单	-/+ 更改设置 <u>Birter</u> 选择子菜单 might (C) 2006-2022 百數软件有限公司	P9 默认值 F10 保存并退出

- SATA 控制器 1 (REAR SATA PORTO CPU1): 打开或关闭 REAR SATA PORTO CPU1 连接的背板上的 Sata Port
- SATA 控制器 2 (SATA PORT0 CPU1 & SATA PORT1 CPU1): 打开或关闭 SATA PORT0 CPU1 和 SATA PORT1 CPU1 连接的背板上的 Sata Port
- SATA 控制器 3 (SATA PORT2 CPU2): 打开或关闭 SATA PORT2 CPU2 连接的 背板上的 Sata Port

# 2.3.4 SATA 设备信息

若光标焦点在"SATA 设备信息"时,当按下"Enter"键,则会进入该子页面,如图 2-15 所示:

#### 图 2-15 SATA 设备信息页面

百然ilgofinre软件U1.0 设备	
SATA设备信息	帮助信息
SATA控制器1 (REAR_SATA PORTO CPUL)         SATA端口1-1       未安装         SATA端口1-2       未安装         SATA控制器2(SATA PORTO CPU1 & SATA PORT1 CPUL)         SATA控制器2(SATA PORTO CPU1 & SATA PORT1 CPUL)         SATA控制器2(SATA PORTO CPU1 & SATA PORT1 CPUL)         SATA控制器2(SATA PORT0 CPU1 & SATA PORT1 CPUL)         SATA控制器2(SATA PORT0 CPU1 & SATA PORT1 CPUL)         SATA控制器2(SATA PORT0 CPU1 & SATA PORT1 CPUL)         SATA端口2-1       未安装         SATA端口2-2       未安装         SATA端口2-4       未安装         SATA端口2-6       未安装         SATA端口2-7       未安装         SATA端口2-8       未安装         SATA端口2-7       未安装         SATA端口3-1       未安装         SATA端口3-1       未安装         SATA端口3-3       未安装         SATA端口3-4       未安装	
	P9 默认值 P16 保存并退出
Copyright (C) 2006-2022,百敖软件有限公司	

- SATA 控制器 1 (REAR SATA PORTO CPU1):显示 REAR SATA PORTO CPU1 连接的背板上所接硬盘信息
- SATA 控制器 2 (SATA PORT0 CPU1 & SATA PORT1 CPU1):显示 SATA PORT0 CPU1 和 SATA PORT1 CPU1 连接的背板上所接硬盘信息
- ▶ SATA 控制器 3 (SATA PORT2 CPU2):显示 SATA PORT2 CPU2 连接的背板上 所接硬盘信息

## 2.3.5 NVME 设备

若光标焦点在"NVME 设备"时,当按下"Enter"键,则会进入该子页面,显示主板 上 NVME 设备信息,如图 2-16 所示:

#### 图 2-16 NVME 设备页面



## 2.3.6 USB 配置

若光标焦点在"USB 配置"时,当按下"Enter"键,则会进入该子页面,如图 2-17 所示:

#### 图 2-17 USB 配置页面



- $\triangleright$
- USB 存储设备支持: 打开或关闭 USB 存储设备的支持, 默认打开  $\geq$
- CPU1 USB 端口:打开或关闭 CPU1 USB 端口的支持,默认打开  $\triangleright$
- CPU2 USB 端口: 打开或关闭 CPU2 USB 端口的支持, 默认打开 ≻
- USB 设备列表:显示接入的 USB 相关设备信息  $\triangleright$

## 2.3.7 PCI 设备信息

若光标焦点在"PCI设备信息"时,当按下"Enter"键,则会进入该子页面,显示当 前 PCI 设备信息,如图 2-18 所示:

#### 图 2-18 PCI 设备信息页面

设备		百然ligoCore软件U1.0	
		PCI设备信息	帮助信息
BUS DEV FUN	厂商ID 设备ID	设备类	
00 00 02	1D94 1451	Base system peripherals	
00 14 00	1D94 790B	SMBus	
01 00 00	8086 1521	Ethernet controller	
01 00 01	8086 1521	Ethernet controller	
01 00 02	8086 1521	Ethernet controller	
01 00 03	8086 1521	Ethernet controller	
03 00 00	14A4 2300	NVMe	
05 00 00	1A03 2000	VGA controller	
06 00 03	1D94 145F	USB XHCI	
07 00 02	1D94 7901	SATA AHCI	
10 00 02	1D94 1451	Base system peripherals	
13 00 03	1D94 145F	USB XHCI	
14 00 02	1D94 7901	SATA AHCI	
20 00 02	1094 1451	Base system peripherals	
30 00 02	1094 1451	Base system peripherals	
40 00 02	1094 1451	Base system peripherals	
41 00 03	1094 145F	USB XHUI	
42 00 02	1094 7901	SHIH HHUI	
50 00 02	1094 1451	Base system peripherals	
51 00 03	1004 1450	USB ANUI	
	1094 1451	Base system peripherals	
70 00 02	1074 1401	Dase system peripherals	
11 00 00	0000 1003	Ethernet controller	
F1 帮助	1. 选项	条目 -/+ 更改设置	F9 默认值
Esc 退出	↔ 选择	菜单 Enter 选择子菜单	F10 保存并退出
		Comuniant (C) 2006-2022, 百數软件有限公司	

# 2.4 高级界面功能描述

该页面显示 CPU C-State 状态、系统调试模式、4GB 以上空间解码、超线程、CPU SVM 控制、CPU P-State 控制、SR-IOV 控制、NUMA、漏桶分钟数、PCIE CE 阈值、 CPU CE 阈值、APEI CPU CE 注错支持,RAS CE Smi 阈值、串口重定向、服务管理、 RTC 唤醒、海光设置和 UEFI HII 配置,则如图 2-19 所示:。

图 2-19 高级页面

主页设备高级安全	白素BgaCore软件01.0 启动退出	
CPU C-State状态	关闭	帮助信息
系统调试模式 <b>4GB</b> 以上空间解码	<打开> <打开>	设定串口调试信息模式。注意:Windows OS默认会禁用串口,如果启用这个功能 Windowe可能会出现短期的不响应。
超线程 CPU SUM控制 CPU P-State控制 SR-IOU支持	(打开) (打开) (打开) (打开)	2 ATIMON OF REALISTING HALL HAVE
NUMA	(打开)	
漏桶分钟数	[0]	
PCIE CE阈值 CPU CE阈值	[1] [4096]	
APEI CPU CE注错支持 RAS CE Smi阈值	<打开> [5]	
<ul> <li>▶ 串口重定向</li> <li>▶服务管理</li> <li>▶ RTC唤醒</li> <li>▶ 海光设置</li> <li>▶ UEFI HII配置</li> </ul>		
E1 帮助 Esc 退出	14 选项条目 -/- 更改设置 14 选择菜单 Cinter 选择子菜单 Committee (C) 2005 - 2022 - 五射软化石	▶9 默认值 ▶10 保存并退出

- ▶ CPU C-State 状态:显示 CPU C-State 状态
- ➤ 系统调试模式:打开或关闭串口调试信息
- ▶ 4GB 以上空间解码:打开或关闭 4GB 以上空间解码
- ▶ 超线程:打开或关闭超线程
- ➢ CPU SVM 控制: 打开或关闭 CPU SVM
- ▶ CPU P-State 控制: 打开或关闭 CPU P-State
- ▶ SR-IOV 支持: 打开或关闭单根 I/O 虚拟化
- ▶ NUMA:打开或关闭 CPU NUMA
- ▶ 漏桶分钟数:设置内存 CE 错误数减少的周期
- ▶ PCIE CE 阈值: 设置 PCIE CE 阈值,范围 0~10000
- ➤ CPU CE 阈值: 设置 CPU CE 阈值,范围 1~4096
- APEI CPU CE 注错支持: 打开或关闭 APEI CPU CE 注错支持
- ▶ RAS CE Smi 阈值: 设置 CE 风暴阈值,范围 5~20
- ▶ 串口重定向:此选项用以设置串口重定向相关配置
- ▶ 服务管理:此选项用以设置服务管理相关配置
- ▶ **RTC 唤醒**: 设置系统启动的星期和时间
- ▶ 海光设置:此选项用以设置海光相关配置
- > UEFI HII 配置: 此选项用以设置和显示 UEFI HII 相关配置

## 2.4.1 串口重定向

若光标的焦点在"串口重定向"时,按下"Enter"键,则会进入串口重定向子页面, 串口重定向默认关闭,如图 2-20 所示:

图 2-20 串口重定向(默认关闭)

高级		百敖ByoCore软件U1.0	
	串口重定向		帮助信息
串口重定向			DOS串口重定向,只支持MS-DOS 7.1及 下版本 不支持Uindows 98 MS-DOS
串口重定向			
P1 帮助 P2 退出	11 选项条目	-/* 更改设置 Parton: 选择子技角	29 默认值 210 保存并退出
	Copyri	ght (C) 2006-2022, 百敖软件有限公司	

若打开串口重定向,则如图 2-21 所示:

图 2-21 串口重定向打开

高级	HX:ByoLore#\1+V1.	Đ.
	串口重定向	帮助信息
串口重定向 串口 重定向 串口波特率 终端类型	<115200> <nutd></nutd>	DOS串口重定向,只支持MS-DOS 7.1及 下版本,不支持Windows 98 MS-DOS
1	11 选项条目 -/* 更改设置	
	Copyright (C) 2006-2022,百敖软	件有限公司

▶ 串口重定向:选择是否打开串口重定向,默认关闭

- ▶ 串口波特率:显示串口波特率(当串口重定向打开才显示),默认 115200
- ▶ 终端类型:选择终端类型(当串口重定向打开才显示),默认 Auto

### 2.4.2 服务管理

若光标焦点在"服务管理"时,按下"Enter"键,则会进入子页面,如图 2-22 所示:

and and an and an and an	百敖BypCore软件V1.0	
服务	· · · · · · · · · · · · · · · · · · ·	帮助信息
BMC自检状态 BMC Firmware版本 IPMI版本	Inaccessible data or device[ 4h 1.4.0 2.0	启用/禁用专用管理局域网的 Lan上串 行功能。
专用SOL ▶ BMC系统日志 清除系统事件日志 ▶ BMC网络配置	<禁用>	
11 帮助 11 选项条目 Bac 退出 ↔ 选择菜单	-/* 更改设置 Enter 选择子菜单	P9 默认值 F10 保存并退出
	Copyright (C) 2006-2022, 百敖软件有限公司	

#### 图 2-22 服务管理信息页面

- ▶ BMC 自检状态:显示 BMC 的自检状态,正常为 PASSED
- ▶ BMC Firmware 版本:显示 BMC 的固件版本号
- ▶ IPMI 版本:显示 IPMI 的版本号,固定为 2.0
- ▶ 专用 SOL: 启用或禁用 SOL 功能,默认禁用
- ▶ BMC 系统日志:此选项可以收集 BMC 系统日志,最多显示最新的 200 条
- ▶ **清除系统事件日志**:此选项可以清除 BMC 系统日志
- ▶ BMC 网络配置:此选项可以查看 BMC 网络配置信息

### 2.4.2.1 BMC 系统日志

若光标焦点在 "BMC 系统日志"时,按下 "Enter"键,则会进入 BMC 系统日志信息子页面,如图 2-23 所示:

#### 图 2-23 BMC 系统日志页面

高级		
	BMC系统日志	帮助信息
系统日志总条数	186	i
2021/04/02 11:37:48 BMC 2021/04/02 11:37:48 BMC 2021/04/02 11:37:48 BMC 2021/04/02 11:37:48 BMC	S#76 O#2 Fan Assert S#72 O#2 Fan Assert S#68 O#2 Fan Assert S#64 O#2 Fan Assert	
2021/04/02 11:37:42 BMC 2021/04/02 11:37:42 BMC 2021/04/02 11:37:42 BMC 2021/04/02 11:37:42 BMC 1020/14/01 201:37:42 BMC	S#102 O#0 Fan Assert S#100 O#0 Fan Assert S#98 O#0 Fan Assert S#96 O#0 Fan Assert	
1970/01/01 08:00:53 BHC 2022/08/16 10:55:37 BHC 2022/08/16 10:55:27 BHC 2022/08/16 10:55:25 BHC	SHOO UHU POWER SUPPLY DEASSERT SH93 OH2 Battery Assert SH80 OH0 Power Unit Assert SH80 OH0 Power Unit Deassert SH80 OH0 Power Unit Assert	
2021/04/01 23:27:53 BMC 2021/04/01 23:27:53 BMC 2021/04/01 23:27:53 BMC 2021/04/01 23:27:53 BMC 2021/04/01 23:27:53 BMC	S#76 0#2 Fan Assert S#72 0#2 Fan Assert S#68 0#2 Fan Assert S#64 0#2 Fan Assert	
2021/04/01 23:27:49 BHC 2021/04/01 23:27:49 BHC 2021/04/01 23:27:49 BHC 2021/04/01 23:27:49 BHC 1970/01/01 06:00:54 BHC	SH102 UND FAN ASSERT SH100 OHO FAN ASSERT SH98 OHO FAN ASSERT SH96 OHO FAN ASSERT SH88 OHO Power Supply Deassert	
1970/01/01 08:00:21 BMC 2022/08/15 18:44:21 BMC 2022/08/15 18:44:13 BMC 2022/08/15 18:44:09 BMC 2022/08/15 18:44:09 BMC	S#93 0#2 Battery Assert S#80 0#0 Power Unit Assert S#80 0#0 Power Unit Deassert S#80 0#0 Power Unit Assert S#80 0#0 Power Unit Assert	
2022/08/13 10:40:48 BHC           門 帮助           除:退出	3000 0m0 ruler unit bedssert       1 选项条目     -/- 更改设置       * 选择菜单     Filter 选择子供	★ 對认值 對10 保存并退出
	Copyright (C) 2006-2022, 日 款 软件	H MCA N

## 2.4.2.2 BMC 网络配置

若光标焦点在"BMC 网络配置"时,按下"Enter"键,则会进入 BMC 网路配置子 页面,如图 2-24 所示:

#### 图 2-1 BMC 网络配置

高级		百族ByoCore软件01.0	
	BMC网络配	<u>業</u>	帮助信息
专用局域网配置         IPv4地址         IPv4地址         IPv6地址模式         IPv6 地址         其享口网络配置         IPv4地址模式         IPv4地址模式         IPv4地址模式         IPv4地址模式         IPv4地址模式         IPv4地址模式         IPv6地址模式         IPv6地址模式         IPv6地址模式         IPv6地址模式         IPv6地址模式         IPv6地址模式         IPv6地址模式         IPv6地址         IPv6         IPv6		〈动志〉 192、168.6.206 255.255.255.0 192、168.6.1 〈定用〉 〈动志〉 0000:0000:0000:0000:0000:0000:0000:00	选择 IMC IP Source.如果是静态,则 可以编辑 IP参数,如果是动态,则这 些字段仅显示,并自动获取 IP地址 (DHCP)。
台 帮助 Kai 退出	11 选项条目 ↔ 选择菜单	-/- 更改设置 Enter 选择子菜单	19 默认值 F10 保存并退出
	Cop	yr iynt (C) 2000-2022,日秋秋作作限公司	

▶ 专用局域网配置:此选项用来查看专用网络设备信息,并且修改专用网络相关功能

▶ 共享口网络配置:此选项用来查看共享网络设备信息,并且修改共享网络相关功能

## 2.4.3 RTC 唤醒

若光标焦点在"RTC唤醒"时,按下"Enter"键,则会进入子页面,设置系统启动的星期和时间,如图 2-25 所示:

#### 图 2-25 RTC 唤醒页面

RTC唤醒         帮助信息.           星期日         <关闭>         选择系统启动的星期和时间。此功能           星期一         <关闭>         港择系统启动的星期和时间。此功能           星期一         <关闭>         常系统从关闭状态中唤醒。	
星期日     く关闭>     选择系统启动的星期和时间。此功律       星期一     く关闭>     将系统从关闭状态中唤醒。	
<ul> <li> 生期三 (关団) </li> <li> 星期四 (关団) </li> <li> 星期六 (关団) </li> <li> 単前((町:分:秒)) (00:00:00) </li> </ul>	功能可
_ Ker 退出 → 选择菜单 _ Knter 选择子菜单 F10 保存并退出	

## 2.4.4 海光设置

若光标焦点在"海光设置"时,按下"Enter"键,则会进入海光设置子页面,如图 2-26 所示:

#### 图 2-26 海光设置页面



海光设置中的选项可以参考 HygonCbsHelp.pdf



HygonCbsHelp.pdf

## 2.4.5 UEFI HII 配置

若光标焦点在"UEFI HII 配置"时,按下"Enter"键,则会进入子页面,如图 2-27 所示:

#### 图 2-27 UEFI HII 配置

百友和pcInte软件U1.0 高级			
UEFI HII配置	帮助信息		
<pre>&gt; Driver Health Manager &gt; Tis Auth Configuration &gt; Intel(R) I350 Gigabit Network Connection - 18:98:A5:81:9A:B1 &gt; Intel(R) I350 Gigabit Network Connection - 18:98:A5:81:9A:B2 &gt; Intel(R) I350 Gigabit Network Connection - 18:98:A5:81:9A:B3 &gt; Intel(R) I350 Gigabit CT Desktop Adapter - 00:18:21:39:CA:78</pre>	List all the Driver Health instances to manage		
▶1     帮助     11     选项条目     -/-     更改设置       ▶∞     退出     ▶     选择菜单     医************************************	19 默认值 F10 保存并退出		

▶ UEFI HII 配置:此选项包括网络以及存储设备配置,具体显示内容依照实际为准

Setup 语言设置为中文时,UEFI HII 配置里许多内容仍为英文,因为大部分外插扩展 卡不支持中文。

## 2.5 安全界面功能描述

该界面用来显示设置管理员密码、设置用户密码、设置密码有效期、开机密码(设置管理员密码后可见)、TPM选择、海光 TPCM、TCG2 配置、硬盘密码、TCM 配置、安全启动和硬盘绑定,如图 2-28 所示:

#### 图 2-2 安全页面 (默认配置下)

主页设备高级安全。	百敖BgoCore软件U1.0 动 退出	
管理员家码	未安姓	帮助信息
日子(公司) 一 一 一 一 一 二 二 二 二 二 二 二 二 二 二 二 二 二	木安装	选择这一项来设定、更改以及删除管理员密码。密码支持字符包括字母、数字以及其它可打印字符。密码区分大小写,支持输入密码长度为6到20。
TPM选择 海光TPCM > TCG2 配置 > 硬盘密码 > TCH 配置 > 安全启动 > 硬盘绑定	<关闭> <关闭>	注意: 输入密码时按Enter键输入空可以删除 密码。密码至少包含大写字母,小写字 母,数字,特殊字符四种类型中的三种 。且不能设定为之前设定过的密码,五 (含)次以内。
P1 帮助 14 Esc 退出 ↔	选项条目 -/* 更改设置 选择菜单 Enter 选择子菜单 Comunicate (C) 2005-2022, 百教软件	的 默认值 ELO 保存并退出 有限公司

- ▶ 设置管理员密码:此选项可以用来设置和删除管理员密码
- ▶ 设置用户密码:此选项可以用来设置和删除用户密码
- ▶ 设置密码有效期:设置密码的有效期(管理员密码设置后才显示)
- 开机密码:此选项用来设置是否开启开机密码(管理员密码设置后才显示)
- **TPM 选择:** 默认关闭,可以选择 CPU 内置 FTPM 或外插 DTPM(SPI)或外插 DTPM(LPC)
- ▶ 海光 TPCM: 打开或关闭海光 TPCM
- ▶ TCG2 配置: 默认显示选项,当选择 FTPM 或 DTPM 并保存重启后,该选项内会显示 当前的 TPM 设备信息,及相关配置
- ▶ 硬盘密码:此选项用以显示和设置硬盘密码(RAID 卡和 SAS 卡上的硬盘不支持), 如果系统中没有连接硬盘,则显示为空
- ▶ **TCM 配置:**显示 Tcm 设备信息
- ▶ 安全启动:此选项可以设置安全启动
- ▶ **硬盘绑定:**选择启动硬盘(RAID 卡和 SAS 卡上的硬盘不支持)

! 注意:

请牢记管理员密码,密码一旦丢失,将无法进入 BIOS 配置界面!

## 2.5.1 设置管理员/用户密码

若光标的焦点在"设置管理员密码/设置用户密码"时,按下"Enter"键,则会进入该 子页面,如错误!未找到引用源。所示:

图 2-29 管理员/用户密码界面

主页设备高级安全。启动	百次	dyoCore软件V1.0	
管理品変码	+ 安港		帮助信息
用户密码	未安装		选择这一项来设定、更改以及删除管理 员密码。密码支持字符包括字母、数字
设置管理员密码 设置用户密码			以及其它可打印字符。密码区分大小写,支持输入密码长度为6到20。
TPM选择 海光TPCM	<关闭> <关闭>		注意: 输入密码时按Enter键输入空可以删除
▶ TCG2 配置			密码。密码至少包含大写字母,小写字 母,数字,特殊字符四种类型中的三种
▶ 硬盈盈的 ▶ TCM 配置 ▶ 安全启动			。且不能设定为之前设定过的密码,五 (含)次以内。
▶ 硬盘绑定		青输入新密码	
	_		
P1 帮助	选项条目 选择菜单	-/* 更改设置 Sinter 选择子菜单	29 默认值 F10 保存并退出
	Copyright (C) 200	06-2022,百敖软件有限公司	

设置管理员密码后,开机密码选项可见,如图 2-30 所示: 图 2-2 开机密码

	主页设备高级安全启动	白和BypCore软件V1. 退出	8
用户密码     本女菜     西井是合井启井机金码切配。       设置管理员密码 设置用户容码 设置预有效期 开机密码     <<	管理员密码	已安装	帮助信息
せいのう 有効明 けいです 有効時 けいです 有効時 すいです その すいです 配置 での 配置 砂密 空码 TON 配置 交 空后 回 可の 配置 交 空后 回 可の 配置 での ののののののののののののののののののののののののののののののの	用 尸 密 码 设置管理员 密 码	禾女装	选择是否开启并机密码功能。
TPH选择 海光TPON       (关雨) (关雨)         TOC2 配置       (关雨)         硬盘密码       TOC1 配置         TOC1 配置       (共雨)         使盘密码       (共雨)         TOC2 配置       (共雨)         使盘密码       (共雨)         使盘缩词       (共雨)         使盘缩词       (共雨)         使盘缩词       (共雨)         使盘缩词       (共雨)         使盘缩词       (日本)         使盘缩词       (日本)         使盘音频量       (日本)         建语子说单       (日本)         建语子说单       (日本)         使用       (日本)         使用       (日本)         使用       (日本)         使用       (日本)         (日本)       (日本) <td>设置用户密码 设置密码有效期 开机密码</td> <td>&lt;长期有效&gt; &lt;关闭&gt;</td> <td></td>	设置用户密码 设置密码有效期 开机密码	<长期有效> <关闭>	
<ul> <li>▶ TCC2 配置</li> <li>▶ 硬盘密码</li> <li>▶ TCN 配置</li> <li>▶ 安全启动</li> <li>▶ 硬盘绑定</li> <li>▶ 硬盘绑定</li> <li>&gt; 硬盘绑定</li> <li>&gt; 硬盘绑定</li> <li>&gt; 医强 帮助</li> <li>● 选项条目</li> <li>● 大· 更改设置</li> <li>● 数以值</li> <li>● 数译菜单</li> <li>● 数字 选出</li> </ul>	TPM选择 海光TPCM	<关闭> <关闭>	
哲 帮助     計 选项条目     → 更改设置     約 默认值       政治     世 选择菜单     政治     予約       政治     世 选择菜单     政治     予約	▶ TCG2 配置 ▶ 硬盘密码 ▶ TCH 配置 ▶ 安全启动 ▶ 硬盘绑定		
計     帮助     11     选项条目     -/-     更改设置     P3     默认值       Exec 退出     +     选择菜单     Exec 选择子菜单     F10     保存并退出			
	F1 帮助	は项条目 -/* 更改设置 好菜単 Enter 选择子菜	19 默认值 单

## 2.5.2 TCG2 配置

若光标的焦点在"TCG2 配置"时,按下"Enter"键,则会进入该子页面,如错误!未 找到引用源。所示:

安全	百敖ByoCore软件V1.0	
TCG2 配	<u> </u>	帮助信息
当前的 TPM 设备 TPM 状态	IPM 2.0 <启用>	TPH 状态控制。当禁用时,将不响应任何 TPM 命令,并且以下选项将被隐藏。
<b>TPM2.0 设备已找到</b> 固件版本 = 供应商 =	0.1616 HYG	
平台Hierarchy 存储Hierarchy 背书Hierarchy PH值随机化	<启用> <启用> <启用> <启用>	
当前的 TPM 设备接口 PTP TPM 设备接口能力	Hygon PSP Hygon PSP	
TPM2 活跃的 PCR 哈希算法 TPM2 硬件支持的哈希算法 BIOS 支持的哈希算法	SM3256 SM3256 SM3256	
TPH2物理状态操作 当前的 PPI 版本 尝试使用的 PPI 版本 TPH2 操作 TPH2 操作参数	1.3 <1.3> <无动作> I0I	
<b>TCG2 协议配置</b> 支持的事件日志格式 哈希算法位图 PCR Banks 数量 活跃的PCR Banks	TCG_2 SM3_256 1 SM3_256	
E1 帮助 11 选项条目 Nac 退出 ↔ 选择菜单 Ca	-	75 默认值 710 保存并退出

#### 图 2-31 TCG2 配置页面

## 2.5.3 硬盘密码

若光标的焦点在"硬盘密码"时,按下"Enter"键,则会进入该子页面,根据当前接入的硬盘显示信息,如图 2-32 所示:

#### 图 2-32 硬盘密码界面

安全	百敖ByoCore软件U1.0	
	硬盘密码	帮助信息.
设置硬盘密码的哈希算法	<sha-256 hash=""></sha-256>	生成硬盘密码的哈希算法:Sha256 or SH3
选择驱动器		
▶ NUME (PCI3-0-0) : LITEON CA3-8D256	(TCG-OPAL)	
	-/- 更改设置  単 -/- 更改设置	四 默认值 F10 保存并退出
	Copyright (C) 2006-2022, 百敖软件	有限公司

#### ▶ **设置硬盘密码的哈希算法:**选择生成硬盘密码的哈希算法,默认 SHA256

若选择了某个硬盘进入后,则会进入该子页面,如图 2-33 所示: 图 2-33 设置硬盘密码前

硬盘密码帮助信息NUME (PC13-0-0): LITEON CA3-80256 (TCG-OPAL)获得NUME (PC13-0-0): LITEON CA3-80256 (TCG-OPAL)请谨慎使用硬盘密码功能。 忘记密码后驱动器将永远无法使用。 设定立即生效,不需要保存。 (系统重启时,如果硬盘掉电,硬盘状态会重置,启动时需要再次输入密码;如硬盘未掉电, ,则硬盘状态保持,无需重新解锁。)密码支持字符包括字母、数字、空格 及持殊可打印字符。密码需要至少包、 一个空格或持殊字符、需要空少包。 写字母、大写字母和数字中的两种。 持输入密码长度为B到32。设置硬盘密码:未安装 启用NUME硬盘管理员密码启用NUME硬盘管理员密码	「安全」 「安全」	百數BypCore软件01.0	
NUHE (PCI3-0-0): LITEUN CA3-8D256 (TCG-OPAL) 请谨慎使用硬盘密码功能, 忘记密码后驱动器将永远无法使用。 设定立即生效,不需要保存。 《系统重启时,如果硬盘掉电,硬盘状态会重置,启动时需要再次输入密码;如硬盘未掉电 ,则硬盘状态保持,无需重新解锁。》 设置硬盘密码:未安装 启用NUHE硬盘管理员密码	硬盘	2码	帮助信息
	NUHE (PCI3-0-0): LITEON CA3-8D256 (TCG-OPF 请谨慎使用硬盘密码功能, 忘记密码后驱动器将永远无法使用。 设定立即生效,不需要保存。 《系统重启时,如果硬盘掉电,硬盘状态会重 ,则硬盘状态保持,无需重新解锁。》 设置硬盘密码:未安装 启用NUME硬盘管理员密码	L) 置,启动时需要再次输入密码;如硬盘未掉电	获得NUME设备所有权,设置并启用硬盘 密码。设备需要关闭电源才能更新安全 状态。 密码支持字符包括字母、数字、空格以 及特殊可打印字符。密码需要至少包含 一个空格或特殊字符,需要至少包含小 写字母、大写字母和数字中的两种。支 持输入密码长度为0到32。
(2) 帮助     (3) 选项条目     (4) 近夜条目     (5) 近夜子菜     (6) 保存并退出     (7) 默认值     (7) 默认值     (7) 就译菜     (7) 近夜子菜     (7) 定分子菜     (7) こ 合分子菜     (7) 定分子菜     (7) 定分子菜     (7) 定分子菜     (7) 定分子菜     (7) こ 合分子菜     (	門     帮助     14     选项条目       Baid     □     选择菜单	-/+ 更改设置 <u>Citier</u> 选择子菜单 onurright (C) 2996-2922. 百數软件有限公司	19 默认值 110 保存并退出

# 若设置完硬盘密码后,"禁用硬盘密码"、"更改硬盘用户密码"、"更改硬盘管理员密码"、"安全擦除硬盘数据"会出现,如图 2-34 所示:

#### 图 2-34 设置硬盘密码后

百秋ilgpCnre软件01.0 安全	
	帮助信息
NUME (PCI3-0-0) : LITEDN CA3-8D256 (TCG-OPAL)	输入硬盘管理员密码,擦除硬盘数据。 按除之后, 研究网与研究内的方田白
安全擦除硬盘数据	操陈之石,硬盖当问与硬盖内所有用户 数据均被清除。擦除时间可能较长,请 等待。
请谨慎使用硬盘密码功能, 忘记密码后驱动器将永远无法使用。 设定立即生效,不需要保存。 (系统重启时,如果硬盘掉电,硬盘状态会重置,启动时需要再次输入密码;如硬盘未掉电 ,则硬盘状态保持,无需重新解锁。)	
设置硬盘密码:已安装	
禁用硬盘密码 更改硬盘管理员密码 更改硬盘管理员密码	
對         帮助         1/2         ● 建设条目         ● //2         ● 更改设置           Exe         退出         ● 选择菜单         ● 1/2	▶9 默认值 ▶18 保存并退出
Copyright (C) 2006-2022, 日放软件有限公司	

➢ 安全擦除硬盘数据:擦除硬盘数据

> 禁用硬盘密码: 输入现有密码之后来删除硬盘密码

> **更改硬盘用户密码:**更改硬盘用户密码,硬盘密码保持启用

▶ **更改硬盘管理员密码:**更改硬盘管理员密码,硬盘密码保持启用

# ✓! 注意:

请牢记硬盘密码,密码一旦丢失,驱动器将无法使用!

## 2.5.4 TCM 配置

若光标的焦点在"TCM 配置"时,按下"Enter"键,则会进入该子页面,显示 TCM 设备信息,如图 2-35 所示:

#### 图 2-35 TCM 配置页面



## 2.5.5 安全启动

若光标的焦点在"安全启动"时,按下"Enter"键,则会进入该子页面,如图 2-36 所示:

#### 图 2-36 安全启动页面

安全			
	安全启动		帮助信息
系统模式 安全启动		设定模式 《关闭》	[打开] 打开安全启动,BIOS 会阻止未 被援权的系统被调起。[关闭] 关闭安 全启动。
恢复出厂设置 重置为设定模式 进入审计模式 进入部署模式		(进入) (进入) (进入)	
▶ 安全设置项管理			
		t <sub>e</sub>	
F1 帮助 Esc 退出	14 选项条目 ↔ 选择菜单	-/+ 更改设置 Enter 选择子菜单	P9 默认值 P10 保存并退出

- ▶ 安全启动:选择安全启动功能是否开启,默认关闭
- ▶ 恢复出厂设置: 若光标的焦点在"恢复出厂设置"时, 按下"Enter"键, 将会把安全 启动重置到出厂默认值
- ▶ 重置为设定模式:若光标的焦点在"重置为设定模式"时,按下"Enter"键,将会重置为设定模式
- ▶ 进入审计模式: 若光标的焦点在"进入审计模式"时, 按下"Enter"键, 将会重新启动并进入审计模式

# ✓!▲ 注意:

#### 从用户模式进入审计模式将会导致 PK 被删除!

- ▶ 进入部署模式: 若光标的焦点在"进入部署模式"时,按下"Enter"键,将会重新启动并进入部署模式
- > 安全设置项管理:选择此项可更改安全设置启动项,如图 2-37 所示

图 2-37 安全设置项管理选项

	女王		
	安全设置项	管理	帮助信息
			注册/删除 PK
▶ PK 选项			
▶ KEK 选项			
▶ DB 选项			
► DBX 选项			
▶ DBT 选项			
		Ν	
		ч	
<u>时</u> 帮助	<b>11日 选项条目</b>	-/- 更改设置	19. 默认值 200
LSC LEIT	四律来早	Litter 匹挥丁米里	110 休什开应出

# 2.6 启动界面功能描述

该界面用来配置启动相关的功能,如用户等待时间、数字锁定键开机状态、启动模式、内置 Shell、网络引导、网络启动重试、网络引导 IP 版本、Http 启动、更改启动顺序 等信息,如图 2-38 所示:

#### 图 2-38 启动页面

主页设备高级安全,	百族UgoCore软件U1 启动 退出	.0
用户等待时间 数字34字键开机 光杰	[5] /tT#\	帮助信息
点动模式 内置Shell	< (仅UEFI) 〈打开〉	等待热键的倒计时秒数。范围是1秒 到20秒。
网络引导 网络启动重试	(打开) [0]	
网络引导IP版本 Http启动	< <b>IPu4&gt;</b> <关闭>	
uppr带于下的工作师序		
● 硬盘驱动器 ● 网络设备		
CD/DUD光驱 USB闪存驱动器		
USB CD/DUD光驱 ▶ 其它		
- 55U 心山 (H	Copyright (C) 2006-2022,百款转	

- 用户等待时间:此选项用以等待热键的倒计时秒数,范围是1秒到20秒,默认值5 秒
- > 数字锁定键开机状态:此选项用以控制数字锁定键的开机状态,默认打开
- ▶ 启动模式: 设此选项用以选择启动模式, 默认仅 UEFI
- ▶ **内置 Shell:** 此选项用以打开或关闭内置 SHELL, 默认打开
- ▶ 网络引导:此选项用以打开或关闭网络引导,默认打开
- > 网络启动重试:此选项用以设置网络启动重试次数
- ▶ 网络引导 IP 版本:此选项用以选择一个网络引导 IP 版本,默认 IPv4
- ▶ Http 启动:此选项用以打开或关闭 Http Boot,默认关闭
- ▶ UEFI 模式下的开机顺序:根据启动模式选择启动顺序,此选项用以选择 UEFI 模式 下设备的启动顺序(启动模式为仅 UEFI 时可见)
- 传统模式下的开机顺序:根据启动模式选择启动顺序,此选项用以选择传统模式下设 备的启动顺序(启动模式为仅 Legacy 时可见)

# ■。

当存在对应启动设备时,才会相应显示设备的启动优先顺序选项。若无对应启动设备,则下方不会显示设备优先启动顺序选项。

## 2.7 退出界面功能描述

该界面用来配置退出 setup 界面和更新 BIOS 相关的功能,有恢复初始值、保存退出、关机、重启、BIOS 固件更新和启动管理器,如图 2-39 所示:

#### 图 2-39 退出页面

主页设备高级安全启动。退出	百熬ByoCore软件V1.8	
恢复初始值		帮助信息
		为每个选项恢复默认值。
重启		
BIOS固件更新 Deta管理器		
	-/* 更改设置	29 默认值 210 伊东并泪山
190 赵山 村 西洋朱早	Copyright (C) 2006-2022, 百敖软件有限公司	印度 体行开巡话

- ▶ **恢复初始值:** 恢复/加载所有设置选项的默认值
- ▶ 保存退出:在保存设定之后退出
- ▶ 关机:关闭系统
- ▶ 重启:重启系统
- ▶ BIOS 固件更新: 可从 U 盘选择文件更新 BIOS 固件
- ▶ 启动管理器:进入启动管理器菜单

# (i)<sub>提示</sub>

在 SETUP 中用 U 盘进行 BIOS 固件更新时,更新的 U 盘文件名只支持英文显示,中 文的不支持,更新的文件应当放在 U 盘根目录中。

- <u>
  八</u>注意
  - BIOS 固件更新过程中,请勿断电或重启!