研 域
YENTEK

用 户 手 册
User Manual

LGA1151 Processor

Z370VM VER:1.0



物 联 网 解 决 方 案 领 航 者
Internet of Things （IOT) Solution Leader

说　明

除列明随产品配置的配件外，本手册包含的内容并不代表本公司的承诺，本公司保留对此手册更改的权利，且不另行通知。对于任何因安装、使用不当而导致的直接、间接、有意或无意的损坏及隐患概不负责。

订购产品前，请向经销商详细了解产品性能是否符合您的需求。本手册所涉及到的其他商标，其所有权为相应的产品厂家所拥有。

本手册内容受版权保护，版权所有。未经许可，不得以机械的、电子的或其它任何方式进行复制。

欲知更多信息，请访问：

研域工控网站：https://www.hanzsung.com/

研域工控技术支持邮箱：sh.fawang@hanzsung.com

研域工控技术支持手机:19129353172（企业微信同号）

研域工控技术支持企业微信号　　研域商城微信号

订购信息

NO.	Model	Processor	Southbridge	Memory	VGA	HDMI	LAN	USB	COM	RS485/422	Power
1	Z370VM VER:1.0	LGA1151	Z370	4*DDR4	1	2	2*I225V	11	6	COM1/2	ATX

以上订购信息供参考，具体请咨询业务，

温馨提示

1、产品使用前,务必请仔细阅读产品说明书。

2、对未准备安装的主板,应将其保存在防静电保护袋中。

3、在从包装袋中拿主板前,应将手先置于接地金属物体上一会儿,以释放身体及手中的静电

4、在使用前,宜将主板置于稳固的平面上。

5、请保持主板的干燥,散热片的开口缝槽是用于通风,避免机箱内的部件过热。请勿将此类开口掩盖或堵塞。

6、在将主板与电源连接前,请确认电源电压值。

7、请将电源线置于不会被践踏的地方,且不要在电源线上堆置任何物件。

8、当您需连接或拔除任何设备前,须确定所有的电源线事先已被拔掉。

9、为避免人体被电击或产品被损坏,在每次对整机、板卡进行拔插或重新配置时,须先关闭交流电源或将交流电源线从电源插座中拔掉。

10、请留意手册上提到的所有注意和警告事项。

11、为避免频繁开关机对产品造成不必要的损伤,关机后,应至少等待 30 秒后再开机。

12、设备在使用过程中出现异常情况,请找专业人员处理。

13、请不要将本设备置于或保存在环境温度高于70℃上,否则会对设备造成伤害。

注意：如果电池换置不当,会产生爆炸的危险。请务必使用同一型号的或者相当类型的且为制造商推荐的电池。

目 录

第一章 产品介绍.....- 5 -
1.1 产品介绍.....- 5 -
1.2 产品规格.....- 5 -

第二章 安装说明.....- 9 -
2.1 主板尺寸图.....- 9 -
2.2 接口位置示意图.....- 10 -
2.3 安装步骤.....- 11 -
2.4 内存安装.....- 11 -
2.5 跳线功能设置.....- 11 -
2.5.1 CMOS 内容清除/保持设置（JBAT1）.....- 11 -
2.5.2 JPW1 跳线设置.....- 12 -
2.6 接口说明.....- 13 -
2.6.1 SATA 接口（SATA1-1,SATA1-2）.....- 13 -
2.6.2 串行接口(COM1、COM2、COM3-6、JP16、JCOM1、JOMP2、COM1_SW1、COM2_SW1).....- 14 -
2.6.3 显示接口(VGA1、HDMI1、JVGA1、J_HDMI1).....- 16 -
2.6.4 音频接口(AUDIO1、FP_AUDIO1).....- 18 -
2.6.5 电源接口(ATXPWR1、ATX12V1).....- 19 -
2.6.6 键盘鼠标接口(J_KBMS1、UK1).....- 20 -
2.6.7 USB 接口和网络接口(UL1、UL2、F_USB1、F_USB2、USB1).....- 21 -
2.6.8 风扇接口(CPUFAN1、SYSFAN1、SYSFAN2、SYSFAN3、SYSFAN4)- 22 -
2.6.9 前置面板接口(FPANEL2).....- 23 -
2.6.10 Mini-PCIE 和 M.2 接口(SSD1、NGFF1、TPM/WIFI、MSATA).....- 24 -
2.6.11 PCIE 和 PCI 接口.....- 25 -
2.6.12 LPT 接口(LPT1).....- 26 -
2.6.13 TPM 接口(TPM1).....- 27 -
2.7 TPM-4COM 小板安装和使用说明.....- 28 -
2.7.1 产品介绍.....- 28 -
2.7.2 产品实物图.....- 28 -

2.7.3 产品尺寸图 - 29 -
2.7.4 接口示意图 - 29 -
2.7.5 串行接口（COM3、COM4、COM5、COM6） - 30 -

第三章 BIOS 程序设定 - 31 -
3.1 BIOS 描述 - 31 -
3.2 BIOS 基本功能设置 - 31 -
3.2.1 进入 BIOS 界面 - 31 -
3.2.2 Main 菜单（BIOS 信息及时间日期） - 32 -
3.2.3 Advance (高级菜单设置) - 33 -
3.2.4 CPU Configurtation(CPU 设置) - 34 -
3.2.5 PTT Configuration (TPM 配置） - 34 -
3.2.6 Tls Auth Configuration(TLS 认证配置) - 35 -
3.2.7 Trusted Computing(可信计算设置) - 35 -
3.2.8 ACPI Settings (ACPI 配置） - 36 -
3.2.9 Miscellaneous Configuration (杂项配置） - 37 -
3.2.10 IT8786 Super IO Configuration (Super IO 配置） - 38 -
3.2.11 Hardware Monitor (硬件侦测） - 39 -
3.2.12 USB Configuration(USB 配置) - 40 -
3.2.13 CSM Configuration(兼容性配置) - 41 -
3.2.14 NVME Configuration(NVME 配置) - 41 -
3.2.15 Chipset 菜单(芯片组设置) - 42 -
3.2.16 Security(安全设置) - 44 -
3.2.17 BOOT(启动设置) - 45 -
3.2.14 Save & Exite(保存和退出) - 45 -

附录 - 46 -
附录一：术语表 - 46 -
附录二：常见故障分析与解决 - 48 -

第一章 产品介绍

1.1 产品介绍

Z370DM主板采用Intel Z370高速芯片组,支持LGA1151架构的6th/7th/8th/9th Intel Core i7/i5/i3 Pentium/celeron处理器,内部集成Intel® HD图形控制器,提供高性能显示输出,支持VGA、HDMI显示输出,且支持独立双显示,提供4条双通道DDR4 DIMM内存插槽,最大支持64GB,集成2个Intel I225V 2.5G千兆网卡,4个SATA 3.0硬盘接口,6个RS232串口,其中COM1/2支持RS232/422/485功能.提供2个Mini-PCIE插槽,1个MSATA,1个WiFi(可选配TPM-4COM扩展4个串口,需搭配支持TPM-4COM的BIOS,默认是WiFi).2个M.2,1个M.2支持SATA,1个M.2支持4G/5G

该主板具有稳定可靠的工业级性能和网络安全管理等优势,更好的满足了目前市场上大多数专业客户的需求,主要应用服务、工业控制、广电媒资后台、监控集中数据器、和其它高性能紧凑型嵌入式产品等。

1.2 产品规格

- 处理器

  支持LGA1151架构的6th/7th/8th/9th Celeron/Pentium/Core™ i3/i5/i7处理器

- 芯片组

  Intel Z370高速芯片组.

- 内 存

  4* DDR4 DIMM内存插槽,支持双通道2666MHz内存，最大64GB

- 显示功能

  集成Intel® HD Graphics图形控制器，1* VGA接口和1* HDMI1.4接口

  支持单独显示、双显模式、扩展模式

- 网络功能

  2* Intel®I225V 2.5G千兆网卡,支持网络唤醒、PXE功能

➢ 音频功能

板载ALC897 高保真音频控制器,支持Mic,Line out

➢ 扩展总线

1* PCIE3.0 x16插槽

3* PCIE3.0 x4插槽

1* PCIE3.0 x1插槽

2* PCI插槽

1* Mini-PCIE插槽,支持WiFi(可选配TPM-4COM扩展4个串口，需搭配支持TPM-4COM的BIOS)

1* M.2,2242/2250,支持4G/5G，内置NANO SIM卡槽

➢ 存储功能

4* SATA 3.0硬盘接口,SATA接口传输速度可达6Gbps

1* MSATA接口,支持Intel协议的SSD,传输速率达6Gbps

1* M.2,2280,支持NVME PCIE x1/SATA自适应

➢ 背板I/O接口

1* PS/2键盘鼠标接口

1* VGA显示接口

1* HDMI显示接口

2*RS232串口(COM1/2支持5V/12V带电功能,COM1/2支持RS232/422/485)

2* USB 2.0接口

4* USB 3.0接口

2* RJ-45千兆网络接口

1* Line out接口(绿色)、1* Mic接口(红色)

➢ 内置接口

1* PS/2键盘鼠标接口 1*6pin排针，与后置PS/2同信号

1* JVGA接口 1*12pin排针，与外置VGA同信号

1* JHDMI接口 2*8pin排针

4* RS232串口 2*5pin排针

1*前置音频接口 2*5pin排针

4*USB 2.0接口 2*5Pin排针

1*USB2.0接口 USB-TYPE A

1*TPM接口 2*8pin排针

1*LPT打印口 2*13pin排针

1*AC上电自动开机功能 1*3pin排针

1*前面板功能按钮和指示灯接口 2*5Pin排针

1*24pin ATX电源输入接口

2*4pin ATX电源输入接口

- 散热系统

  1*4pin CPU智能风扇接口,4*4pin系统智能风扇接口

- BIOS

  64Mb Flash ROM

- Watchdog功能

  支持硬件复位功能(256级，0~255秒)

- 电源特性

  采用24Pin ATX电源供电

- 操作系统

  Windows 7 / 10 / Linux

- 尺寸、环境

  主板尺寸：305mm x245mm

  工作温度：-10℃～60℃

  工作湿度：5～90%相对湿度,无冷凝

  贮存温度：-20℃～70℃

➢ 实物图

如下：



图一： Z370VM VER:1.0 正面图



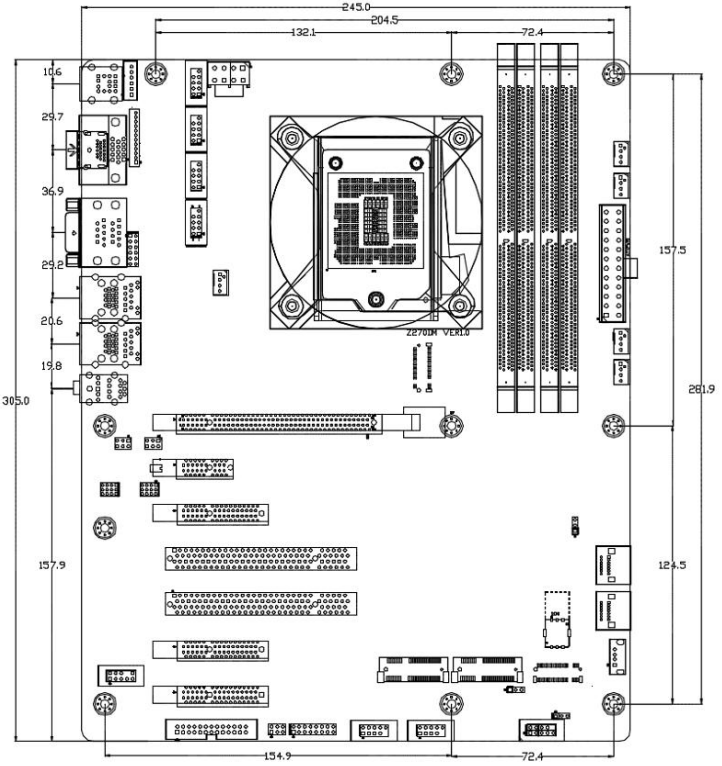
图二：Z370VM VER:1.0 I/O 图

第二章 安装说明

2.1 主板尺寸图

下图为 Z370VM 的正面接口位置和尺寸图。在安装设备的过程中必须小心，对于有些部件，如果安装不正确，它将不能正常工作。

注意：操作时，请戴上静电手套，因为静电有可能会损坏部件。



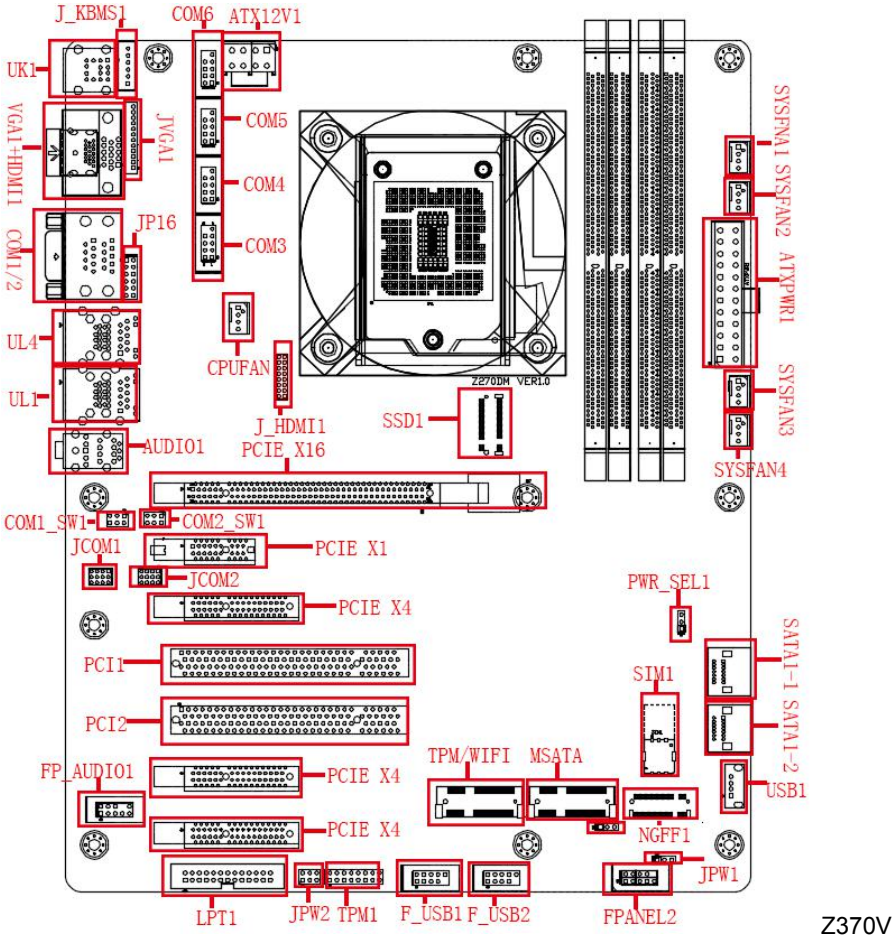
Z370VM VER:1.0 尺寸图

提示:

1.请务必选择合适的螺钉和使用正确的安装方法，否则可能损坏主板。

2.如何识别跳线、接口的第1针脚，观察插头插座旁边的文字标记，会用三角符号或“1”或加粗的线条表示；看背面的焊盘，方型焊盘为第1针脚，在插设备与连接线时注意区分第一脚，否则会损坏主板。

2.2 接口位置示意图



Z370V M VER:1.0 接口位置图

提示：

如何识别报警声:(长鸣声为系统内存出错；短“嘀”一声为开机声)。

2.3 安装步骤

请依照下列步骤组装您的电脑：

1．参照用户手册将 Z370VM 上所有 Jumper（跳线帽）调整正确。

2．安装其他扩展卡。

3．连接所有信号线、电缆、面板控制线路以及电源供应器。

4．启动计算机，完成 BIOS 程序的设置。

⚠本主板关键元器件都是集成电路，而这些元件很容易因为遭受静电的影响而损坏。因此，请在正式安装主板之前，请先做好以下的准备：

1．拿主板时手握板边，尽可能不触及元器件和插头插座的引脚。

2．接触集成电路元件（如 CPU、RAM 等）时，最好戴上防静电手环/手套。

3．在集成电路元件未安装前，需将元件放在防静电垫或防静电袋内。

4．在确认电源的开关处于断开位置后，再插上电源插头。

2.4 内存安装

本主板配有 4 条 DIMM 插槽。安装内存条时请注意以下两点：

1．安装时，将内存条的缺口与插槽的缺口对齐后在用力插紧。

2．选择内存条时必须选择支持本主板规格的内存条。

2.5 跳线功能设置

在进行硬件设备安装之前请根据下表按照您的需要对相应的跳线进行设置。

提示：如何识别跳线、接口的第 1 针脚，观察插头插座旁边的文字标记，会用“1”或加粗的线条或三角符号表示；看看背面的焊盘，方型焊盘为第 1 针脚；所有跳线的针脚 1 旁都有 1 个白色箭头。

2.5.1 CMOS 内容清除/保持设置（JBAT1）

CMOS 由板上钮扣电池供电。清 CMOS 会导致永久性消除以前的系统设置并将其设为原始（出厂设置）系统设置。

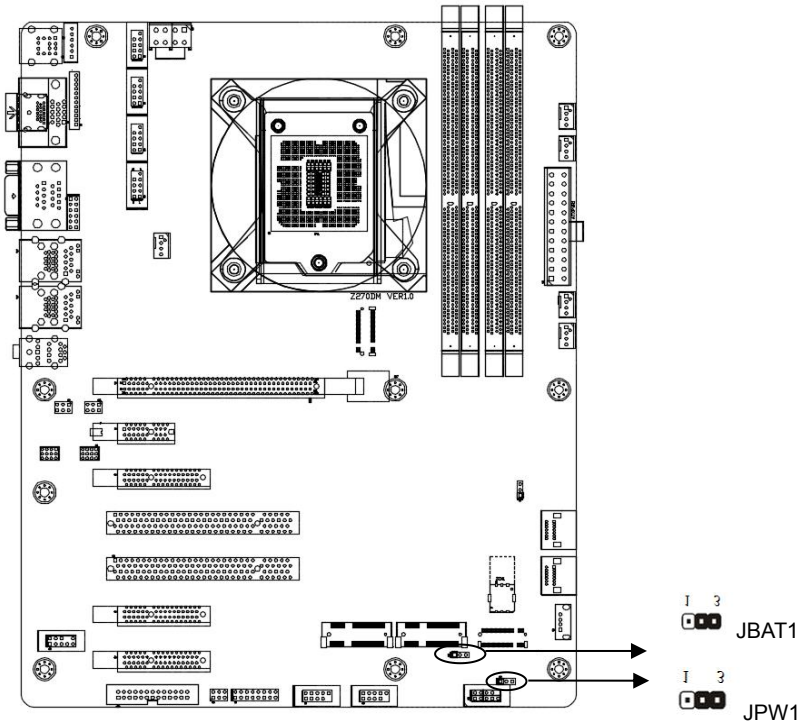
其步骤：(1)关闭计算机，断开电源；

(2)使用跳线帽短接“JBAT1”管脚 2 和 3 短接 5~6 秒，然后还原为 1-2；

(3)开机按键盘中的“Delete”键进入 BIOS 界面；

(4)进入 BIOS 界面按“F9”键----“回车”重载最优缺省值；

(5)按 F10 保存并退出设置。



JBAT1 定义：

设置	JBAT1
短接 1-2 pin	正常工作状态
短接 2-3 pin	清除CMOS内容，所有BIOS设置恢复成出厂值

⚠**请不要在计算机带电时清除 CMOS，以免损坏主板！**

2.5.2 JPW1 跳线设置

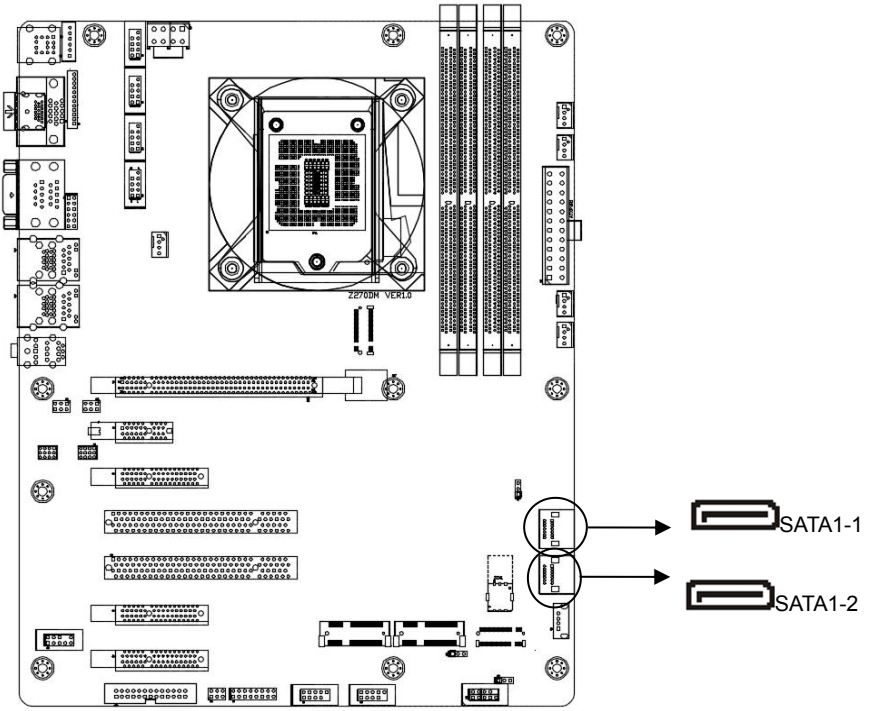
设置	JPW1
短接 1-2 pin	关闭来电自启功能
短接 2-3 pin	打开来电自启功能

2.6 接口说明

⚠连接外部连接器时请先认真阅读本手册，以免对主板造成损坏！

2.6.1 SATA 接口（SATA1-1,SATA1-2）

板上提供 4 个 SATA 3.0 接口,传输速率达 6Gbps.

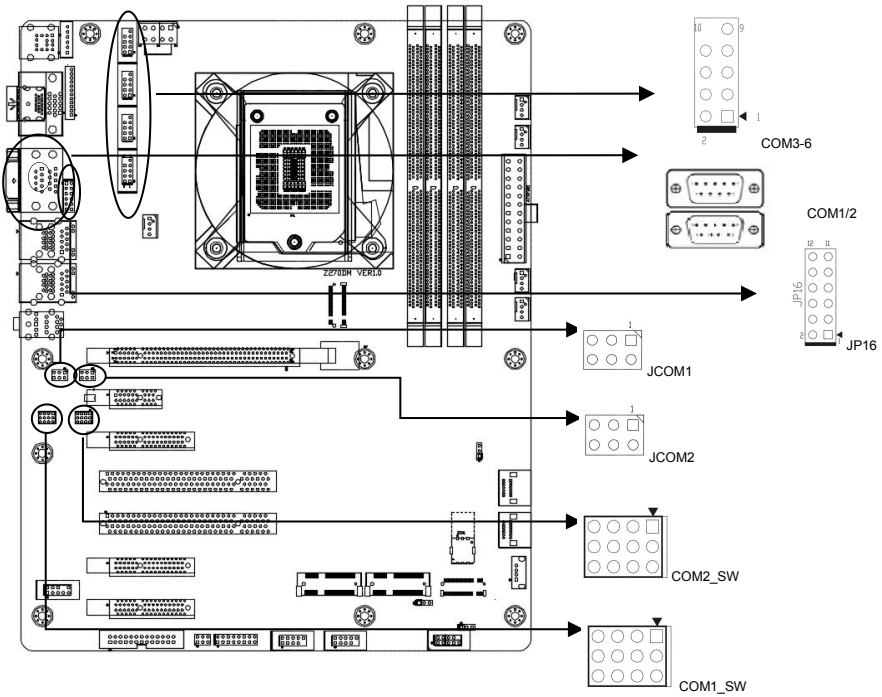


SATA2~6 定义：

管脚	信号名称
1	GND
2	SATA_TXP
3	SATA_TXN
4	GND
5	SATA_RXN
6	SATA_RXP
7	GND

2.6.2 串行接口(COM1、COM2、COM3-6、JP16、JCOM1、JOMP2、COM1_SW1、COM2_SW1)

该板提供6个RS232,其中COM1/2为DB9串口,COM3-6为2*5pin插针,你可在BIOS中开启或关闭串口,并且能够选择其中断IRQ和I/O地址.其中COM1/2支持5V/12V带电功能.COM1/2还支持RS422/485传输模式,可以通过设置跳线来选择,详细设置参阅JCOM1,JCOM2,COM1-SW1,COM2-SW1,JP16跳线设置



COM1、COM2定义：

管脚	RS232	RS422	RS485
1	DCD	TX+	DATA+
2	RX	TX-	DATA-
3	TX	RX+	NC
4	DTR	RX-	NC
5	GND	GND	GND
6	DSR	NC	NC
7	RTS	NC	NC

8	CTS	NC	NC
9	RI	NC	NC

COM3-6 定义:

管脚	信号名称	管脚	信号名称
1	DCD	2	RXD
3	TXD	4	DTR
5	GND	6	DSR
7	RTS	8	CTS
9	RI	10	NC

JP16 设置

设置	功能(JP16)	
短接1-2 pin	RS232	COM1
短接3-4 pin	+5V	
短接5-6 pin	+12V	
短接7-8 pin	RS232	COM2
短接9-10 pin	+5V	
短接11-12 pin	+12V	

JCOM1、JCOM2(COM1/2 RS485/422)设置：

设 置	功 能（JCOM1/2）	
短接 1-2 pin	RS232	COM1/2
短接 3-4 pin	R485	
短接 5-6 pin	R422	

COM1_SW1、COM2_SW1 设置:

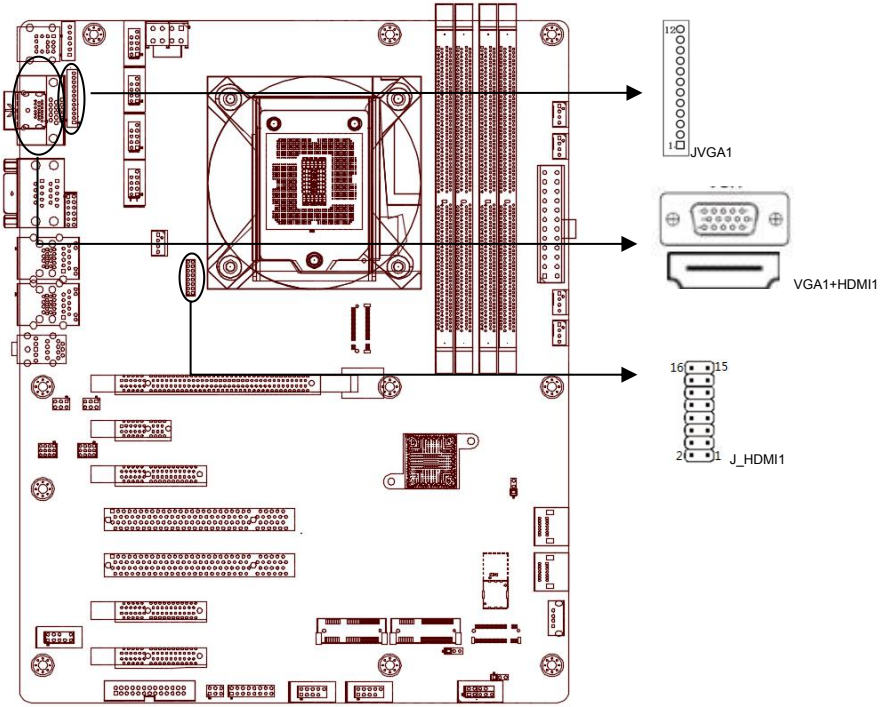
	RS485/422	RS232
COM1_SW1	短接1-2,4-5,7-8,10-11pin	短接2-3,5-6,8-9,11-12 pin
COM2_SW2	短接1-2,4-5,7-8,10-11pin	短接2-3,5-6,8-9,11-12 pin

2.6.3 显示接口(VGA1、HDMI1、JVGA1、J_HDMI1)

主板提供 1 个标准的 VGA 接口,1 个标准的 HDMI 接口

内置 1 个 JVGA 接口,1*12pin 排针，1 个 JHDMI 接口,2*8pin 排针

Note:VGA 与 JVGA1 为同信号, HDMI 和内置 J_HDMI1 排针可以单独使用



VGA1 定义：

管脚	信号名称	管脚	信号名称
1	Red	2	Green
3	Blue	4	NC
5	GND	6	GND
7	GND	8	GND
9	NC	10	GND
11	NC	12	DDCDATA
13	HSYNC	14	VSYNC
15	DDCCLK		

JVGA1 定义：

管脚	信号名称	管脚	信号名称
1	VCC5	2	VSYNC
3	HSYNC	4	GND
5	R	6	GND
7	G	8	GND
9	B	10	GND
11	DDC_SDA	12	DDC_SCL

HDMI 定义：

管脚	信号名称	管脚	信号名称
1	TMDS Data2+	2	TMDS Data2 Shield
3	TMDS Data2-	4	TMDS Data1+
5	TMDS Data1 Shield	6	TMDS Data1-
7	TMDS Data0+	8	TMDS Data0 Shield
9	TMDS Data0-	10	TMDS Clock+
11	TMDS Clock Shield	12	TMDS Clock-
13	Reserved(N.C.)	14	Reserved(N.C.)
15	SCL	16	SDA
17	DDC/CEC Ground	18	+5V Power
19	Hot Plug Detect		

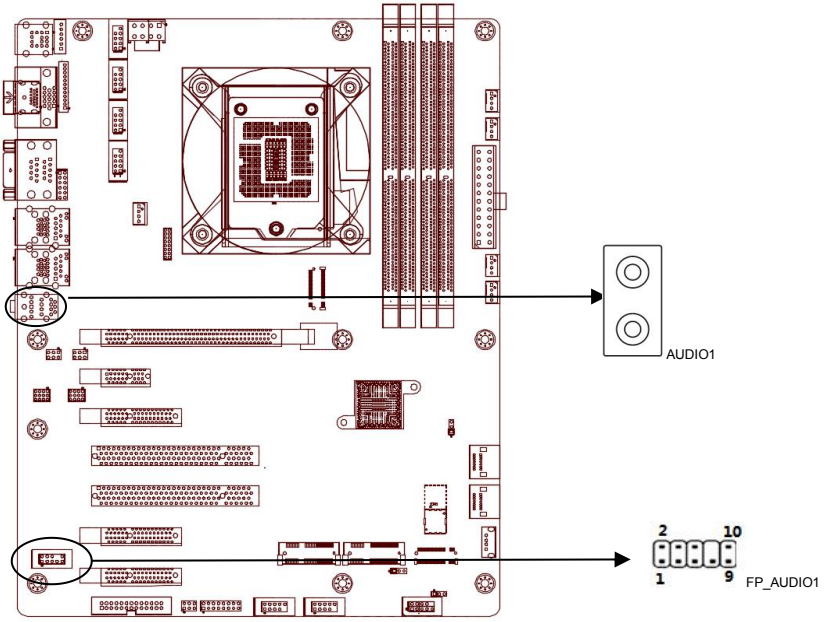
J_HDMI1 定义：

管脚	信号名称	管脚	信号名称
1	TMDS Data2+	2	SCL
3	TMDS Data2-	4	SDA
5	TMDS Data1+	6	NC
7	TMDS Data1-	8	Hot Plug Detect
9	TMDS Data0+	10	+5V Power
11	TMDS Data0-	12	GND
13	TMDS Clock+	14	GND
15	TMDS Clock-	16	GND

2.6.4 音频接口(AUDIO1、FP_AUDIO1)

板上提供一个 AUDIO1 音频插孔,支持 Line out,Mic

内置一个 2*5pin 前置音频接口。

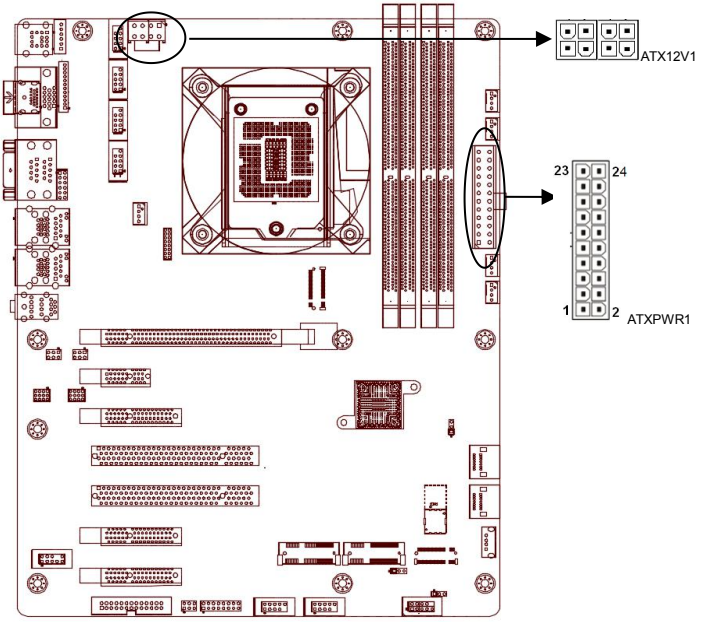


FP_AUDIO1（前置音频）定义:

管脚	信号名称	管脚	信号名称
1	MIC-L	2	GND
3	MIC-R	4	DET
5	Line out-R	6	Sense Return1
7	Sense-FB	8	NC
9	Line OUT-L	10	Sense Return2

2.6.5 电源接口(ATXPWR1、ATX12V1)

板上提供 1 个标准的 24pinATX 电源接口和一个 8pin ATX 电源接口。



ATX12V1 定义：

管脚	信号名称	管脚	信号名称
1	GND	2	12V
3	GND	4	12V
5	GND	6	12V
7	GND	8	12V

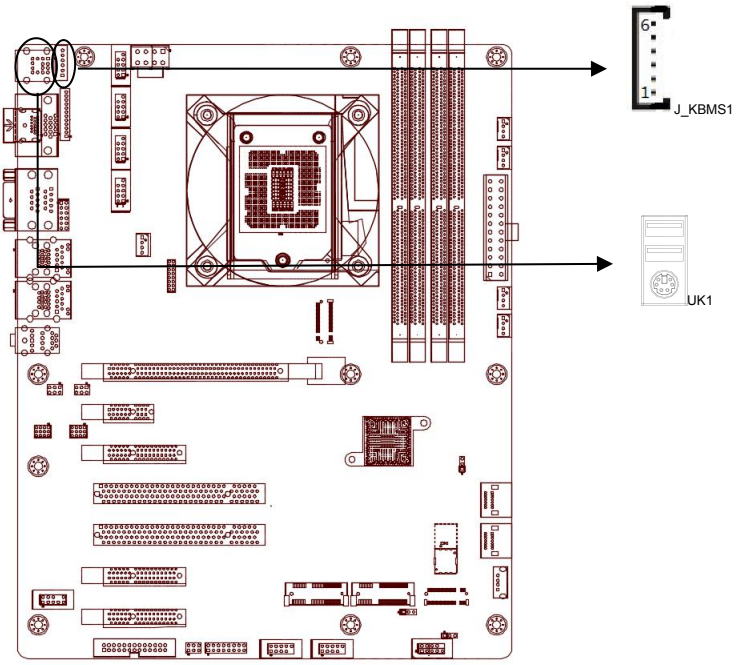
ATXPWR1 定义：

管脚	信号名称	管脚	信号名称
1	3_3V	2	3_3V
3	GND	4	5V
5	GND	6	5V
7	GND	8	PW_OK
9	5VSB	10	12V
11	12V	12	3.3V

13	3_3V	14	-12V
15	GND	16	PS_ON
17	GND	18	GND
19	GND	20	-5V
21	5V	22	5V
23	5V	24	GND

2.6.6 键盘鼠标接口(J_KBMS1、UK1)

板上提供 1 个标准的 PS2 键盘鼠标接口,1 个 1*6Pin 鼠标键盘插针接口,使用时需要用转接线转换成定义中的 PS/2 键盘鼠标接口。



J_KBMS1 接口定义:

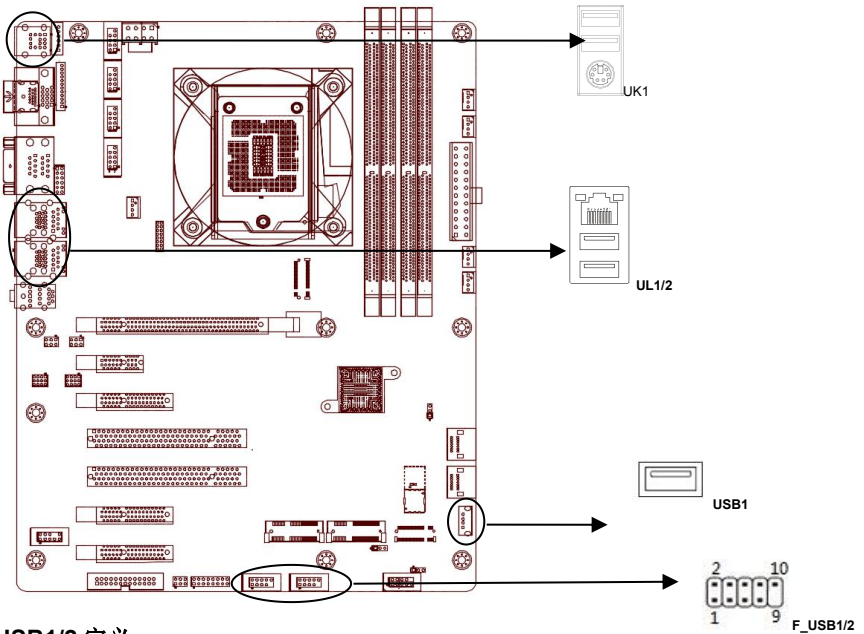
管脚	信号名称	管脚	信号名称
1	MS-CLK	2	VCC
3	GND	4	MS-DATA
5	KB-DATA	6	KB-CLK

2.6.7 USB 接口和网络接口(UL1、UL2、F_USB1、F_USB2、USB1)

分别提供 2 个 USB2.0 接口，4 个 USB3.0 接口，

内置提供 4 个 USB 2.0 接口(2*5pin 2.54mm),1 个 USB2.0 TYPE A 接口

板上提供 2 个标准千兆网络接口

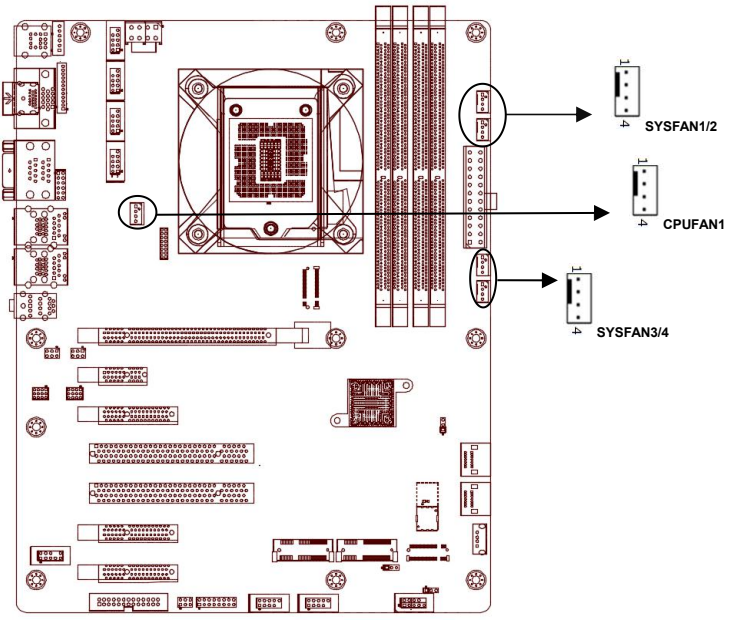


F_USB1/2 定义:

管脚	信号名称	管脚	信号名称
1	VCC	2	VCC
3	D0-	4	D1-
5	D0+	6	D1+
7	GND	8	GND
9		10	GND

2.6.8 风扇接口(CPUFAN1、SYSFAN1、SYSFAN2、SYSFAN3、SYSFAN4)

内置 1 个 4pin CPU 智能风扇接口,4 个 4pin 智能系统风扇接口,



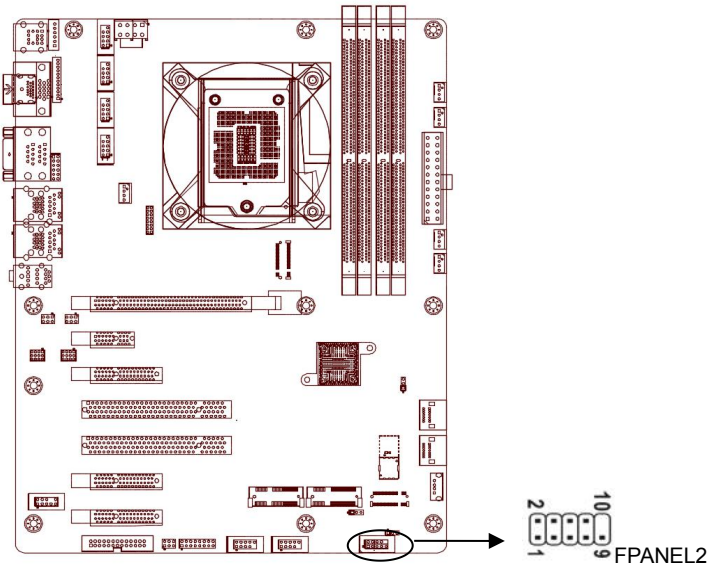
CPUFAN1、SYSFAN1、SYSFAN2、SYSFAN3、SYSFAN4 定义：

管脚	信号名称	管脚	信号名称
1	GND	2	+12V
3	DET	4	PWM

注：DET：风扇转速侦测；PWM：风扇转速 PWM 控制

2.6.9 前置面板接口(FPANEL2)

提供一个2*5pin前面板插针,用于连接至机箱前面板上所设的功能按钮和指示灯.



FPANEL1 定义:

管脚	信号名称	管脚	信号名称
1	HDDLED+	2	PWRLED+
3	HDDLED-	4	PWRLED-
5	GND	6	PWRBTN
7	RESET	8	GND
9	NC	10	

（1）硬盘指示灯（第1，3针HDD LED 第1针为LED的正极）硬盘在进行读写操作时，指示灯便会闪烁，表示硬盘正在运行中。

（2）电源指示灯（第2，4针POWERLED 第2针为LED的正极），当系统接通电源时，电源指示灯亮；当系统断电后，电源指示灯灭。

（3）复位按钮（第5，7针RESET）系统发生故障不能继续工作时，复位可使系统重新开始工作。

（4）电源开关控制（第6，8针POWER BUTTON）这两个引脚连接到机箱前面板上的弹跳开关，可以用来接通或断开电源。

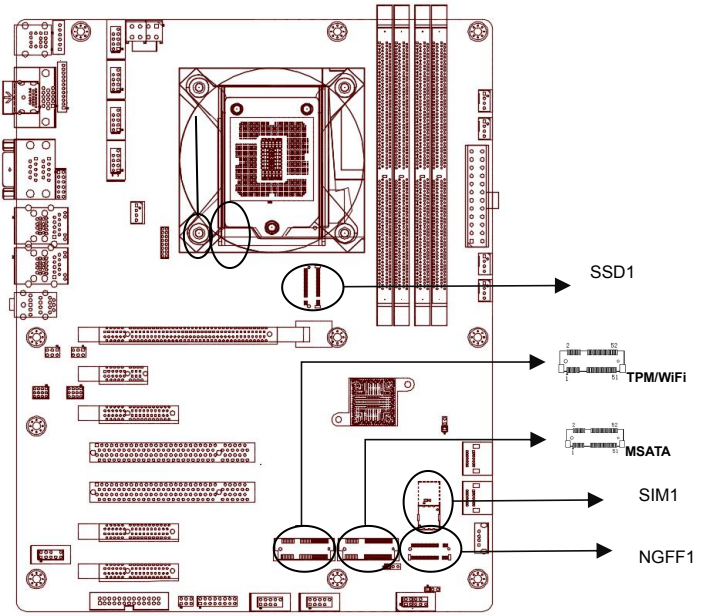
2.6.10 Mini-PCIE 和 M.2 接口(SSD1、NGFF1、TPM/WIFI、MSATA)

主板内置提供1个MSATA插槽,支持Intel协议SSD,传输速度高达6Gbps.

提供1个Mini-PCIE插槽,支持WiFi(可选配TPM-4COM扩展4个串口.需搭配对应的BIOS)

提供1个M.2 2242/2250 4G/5G,1个NANO SIM卡槽

提供1个M.2 2280 支持SATA SSD



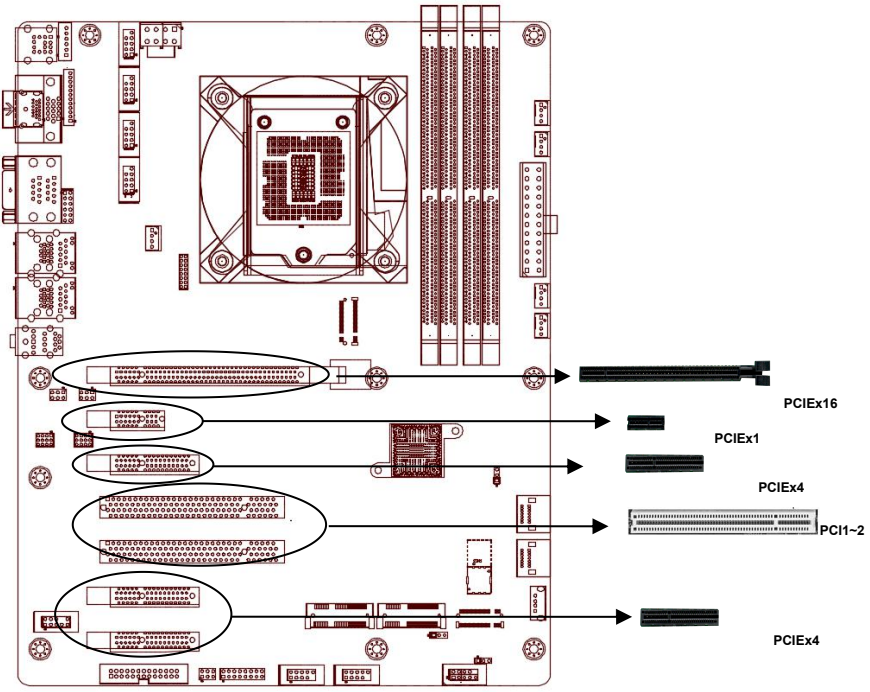
2.6.11 PCIE 和 PCI 接口

提供 1 个标准 PCIE3.0 x16 插槽

提供 3 个标准 PCIE3.0 x4 插槽

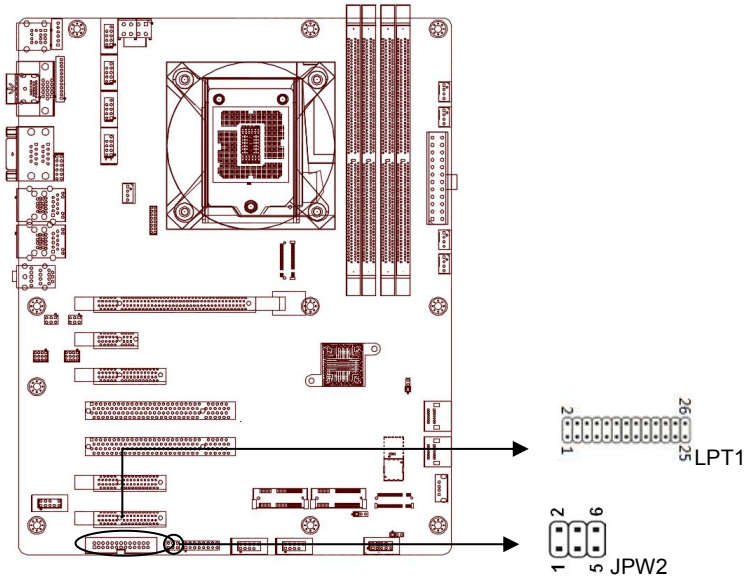
提供 1 个标准 PCIE3.0 x1 插槽

提供 2 个标准 PCI 插槽



2.6.12 LPT 接口(LPT1)

板上提供1个LPT接口 2*13pin排针,默认LPT打印接口，可通过JPW2跳帽选择LPT和GPIO功能，



LPT1 定义：

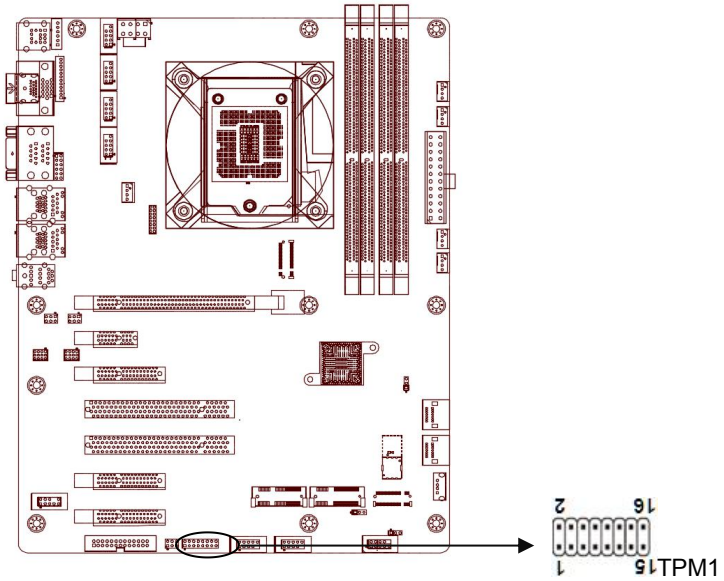
管脚	信号名称	管脚	信号名称
1	STB	2	AFD-
3	PD0	4	ERR-
5	PD1	6	INIT-
7	PD2	8	SLIN-
9	PD3	10	GND
11	PD4	12	GND
13	PD5	14	GND
15	PD6	16	GND
17	PD7	18	GND
19	ACK	20	GND
21	BUSY	22	GND
23	PE	24	GND
25	SLCT	26	NC

JPW2 设置

功 能（LPT1）	设 置
LPT 接口(默认)	短接 3-5, 4-6 pin
GPIO(GPIO 配置需搭配 BIOS)	短接 1-3, 2-4 pin

2.6.13 TPM 接口(TPM1)

板上提供 1 个 TPM 接口 2*5pin 排针



TPM1 定义

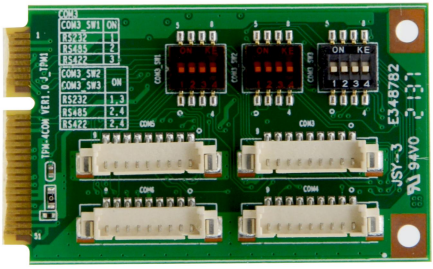
管脚	信号名称	管脚	信号名称
1	CLK_TPM_24M	2	GND
3	LFRAME	4	5VSB
5	PLTRST	6	+5V
7	LAD3	8	LAD2
9	+3.3V	10	LAD1
11	LAD0	12	GND
13	SMB_CLK	14	SMB_DATA
15	3VSB	16	SERIRQ

2.7 TPM-4COM 小板安装和使用说明

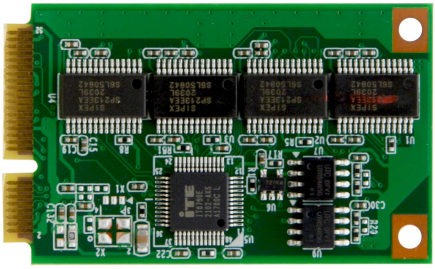
2.7.1 产品介绍

TPM-4COM 为功能扩展板,可以转接 4 个串行接口,其中 COM3 支持 RS485/422 功能,此扩展板可使用在我司带 TPM 接口的主板上

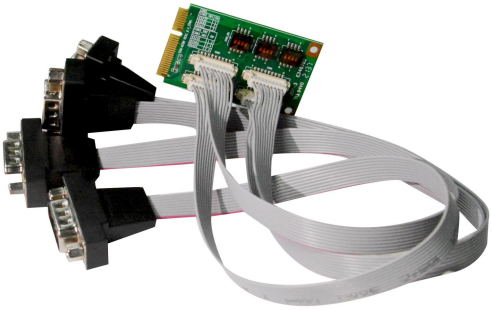
2.7.2 产品实物图



图一： TPM-4COM VER:1.0 产品正面图



图二：TPM-4COM VER:1.0 产品背面图

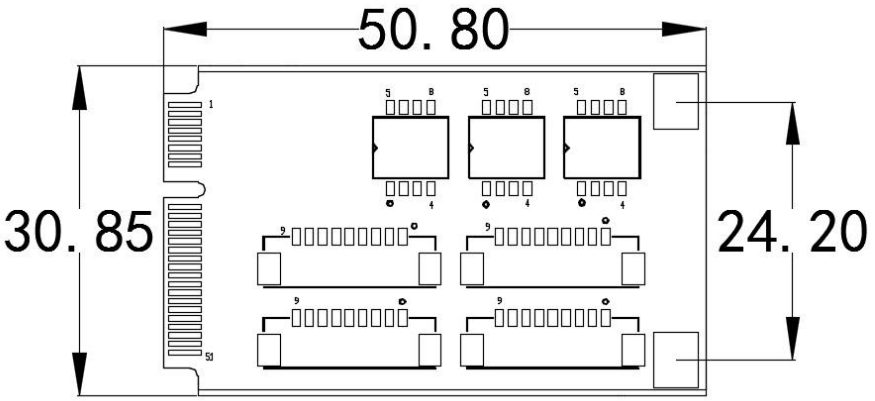


图三：TPM-4COM VER:1.0 带 COM 线

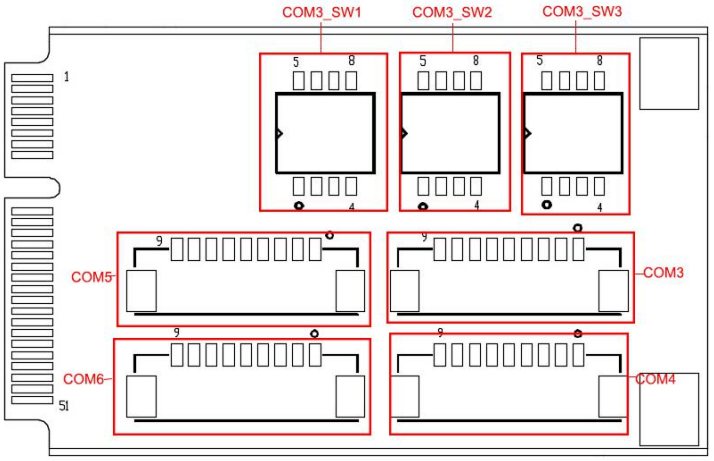
2.7.3 产品尺寸图

下图为 TPM-4COM VER:1.0 的正面接口位置和尺寸图。在安装设备的过程中必须小心，对于有些部件，如果安装不正确，它将不能正常工作。

注意：操作时，请戴上静电手套，因为静电有可能会损坏部件。

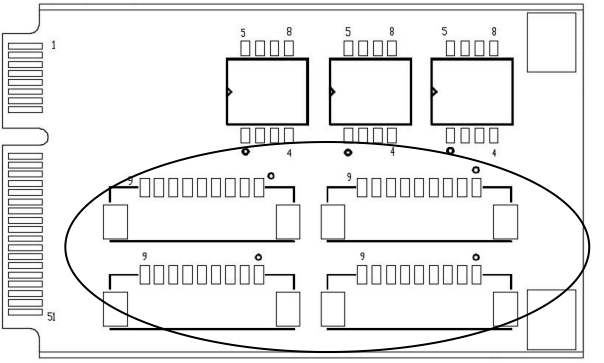


2.7.4 接口示意图



2.7.5 串行接口（COM3、COM4、COM5、COM6）

板上提供 4 个 RS232 串口,1*9pin,PH=1.25mm,其中 COM3 支持 RS485/422 功能



COM3-6

COM3、COM4、COM5、COM6 定义:

管脚	信号名称	管脚	信号名称
1	COM_DCD-_CN	2	COM_RXD_CN
3	COM_TXD_CN	4	COM_DTR-_CN
5	GND	6	COM_DSR-_CN
7	COM_RTS-_CN	8	COM_CTS-_CN
9	COM_RI-_CN		

第三章 BIOS 程序设定

3.1 BIOS 描述

BIOS（Basic Input and Output System，基本输入输出系统），经由主板上的CMOS晶片，记录着系统各项硬件设备的设定参数。BIOS包含了BIOS设定程式，供使用者按照需要自行设置系统参数，使主板正常工作或执行特定的功能。

通过BIOS Setup设置程序修改的相关设置（除了日期、时间）都保存在系统中的闪存存储器中，记忆CMOS资料所需的电力由主板上的电池供应，因此当系统电源关闭时，这些资料不会丢失，当下次再开启电源时，系统便能读取这些设定好的资料。在因误操作无法进入Setup界面时，如需恢复出厂设置，请短接JBAT1 2，3脚清除CMOS内容。

注意！

1. BIOS的设置直接影响到电脑的性能，设置错误的参数将造成电脑的损坏，甚至不能开机，请使用BIOS内置缺省值来恢复系统正常运行。

由于本公司不同产品其设置界面也会略有不同，以下的画面供您参考，有可能跟您目前所使用的BIOS设置程序不完全相同。

3.2 BIOS 基本功能设置

3.2.1 进入 BIOS 界面

按照以下步骤进入BIOS界面

1、启动电源，显示器屏幕将出现POST界面。

2、当屏幕出现”Press<DEL>or<ESC> to enter setup”提示时，按下<DEL>或者<ESC>键，就可以进入BIOS设定程序。

3、以方向键< ↑ >< ↓ >< ← >< → >移动至你要修改的选项，按下<Enter>键即可进入该选项的子画面。

4、使用方向键及<Enter>键即可修改所选项目的值，按回车键选择BIOS选项并修改。

5、使用<Esc>退出主菜单且不保存更改,子菜单退出当前页面并返回主菜单

6、<Page Up/+> 增加数字值或更改

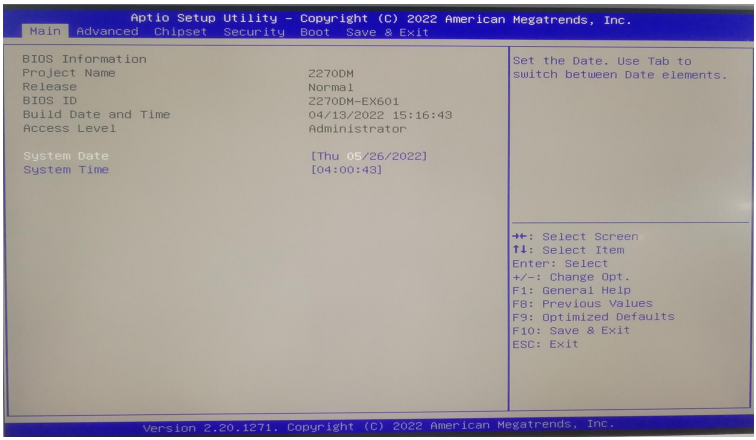
<Page Down/-> 减少数字值或更改

<F1> 设置子菜单帮助

<F9> 设置为默认值(优化成出厂设置)

<F10> 保存BIOS设置

3.2.2 Main 菜单（BIOS 信息及时间日期）



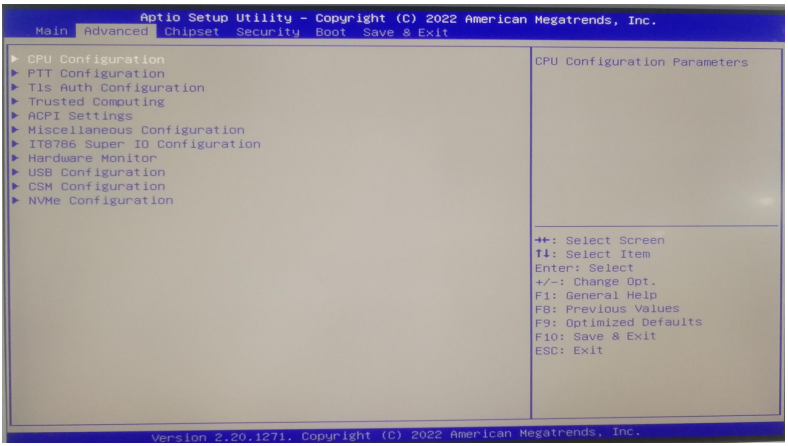
BIOS ID:BIOS版本

Build Date and Time:BIOS时间日期

System Date:设置日期,以月/日/年的格式来表示,其设置范围是：Month/月(Jan.-Dec.)，Date/日(01-31)，Year/年(最大至 2099)。

System Time:设置时间,以时/分/秒的格式来表示。其设置范围是：Hour/时(00-23)，Minute/分(00-59)，Second/秒(00-59)。

3.2.3 Advance (高级菜单设置)



CPU Configuration:CPU 参数信息及常用设置选项

PTT Configuration: TPM设置

TIs Auth Configuration: TLS认证配置

Trusted Computing: 可信计算设置

ACPI Settings:高级配置和电源管理接口设置

Miscellaneous Configuration:杂项配置

IT8786 Super IO Configuration:Super IO 配置信息，包含COM 口中断号及地址设置

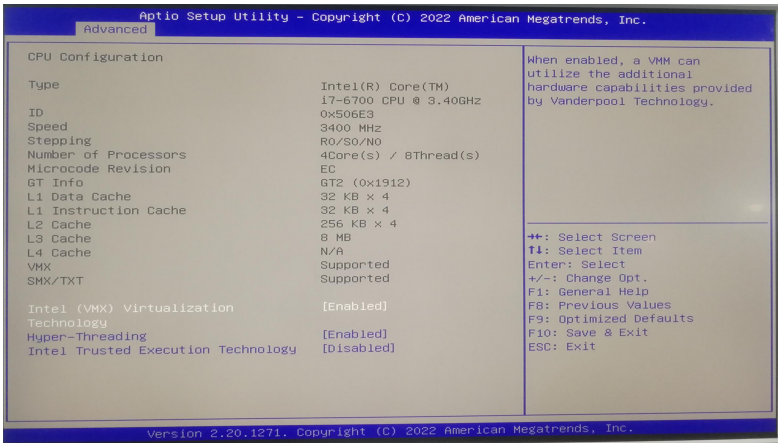
Hardware Monitor: 硬件监视器

USB Configuration: USB配置

CSM Configuration:兼容性设置

NVME Configuration: NVME配置

3.2.4 CPU Configurtation(CPU 设置)



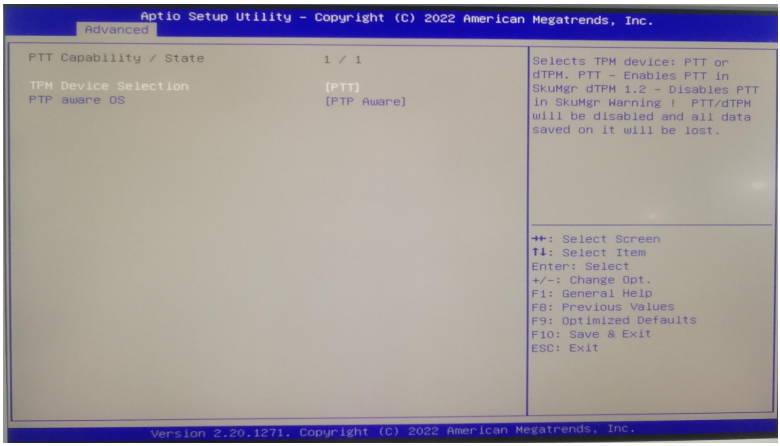
包含CPU的详细信息，CPU厂家、型号、频率、一级缓存大小、二级缓存大小等信息。

Intel (VMX) Virtualization Technology:Intel的虚拟化技术。让硬件平台可以同时运行多个操作系统。

Hyper-Threading:超线程技术，让一颗实体处理器在操作系统内作为两个逻辑处理器

Intel Trusted Execution Techonology: 英特尔可信执行技术,主要用于解决启动进程完整性验证和提供更好的数据保护。

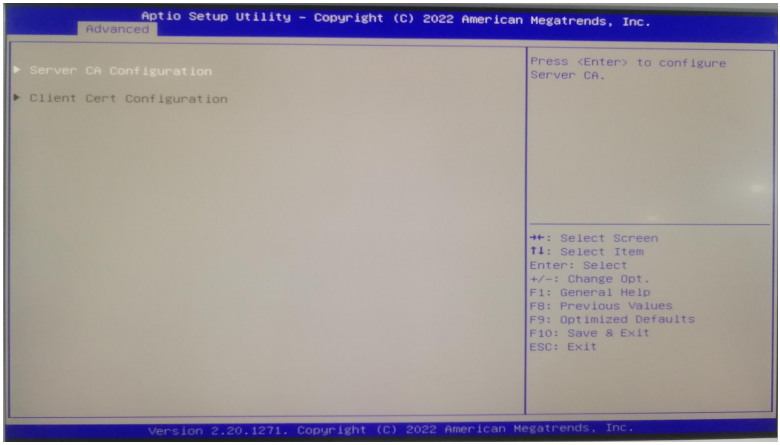
3.2.5 PTT Configuration (TPM 配置）



TPM Device Selection：PTT固件TPM,没有实物，可以理解为“软件TPM”,dTPM没有集成硬件TPM，预留TPM芯片接口

PTP aware OS:默认PTP Aware

3.2.6 Tls Auth Configuration(TLS 认证配置)

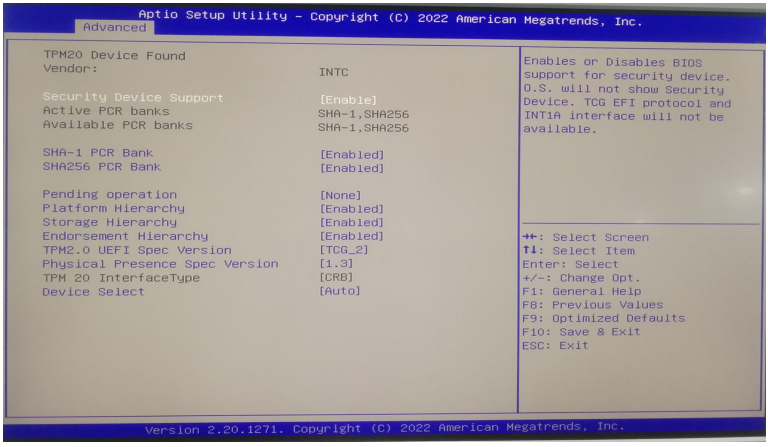


Server CA Configuration：服务器端CA证书配置菜单

Enroll Cert:导入证书接口

Delete Cert:删除证书接口

3.2.7 Trusted Computing(可信计算设置)



Sccurity Device Support:对安全设备的支持，默认Enable

Active PCR BANKS:显示正在使用的PCR BANKS

Availible PCR BANKS:显示可用的PCR BANKS

SHA-1PCR Bank:SHA-1 PCR Bank 启用配置，默认Enabled

SH256 PCR Bank:SHA256 PCR Bank启用配置，默认Enabled

Pending operation:控制设备的安全操作，默认None

Platform Hierarchy:平台等级开关，默认Enabled

Storage Hierarchy:存储等级开关，默认Enabled

Endorsement Hierarchy:认可等级开关，默认Enabled

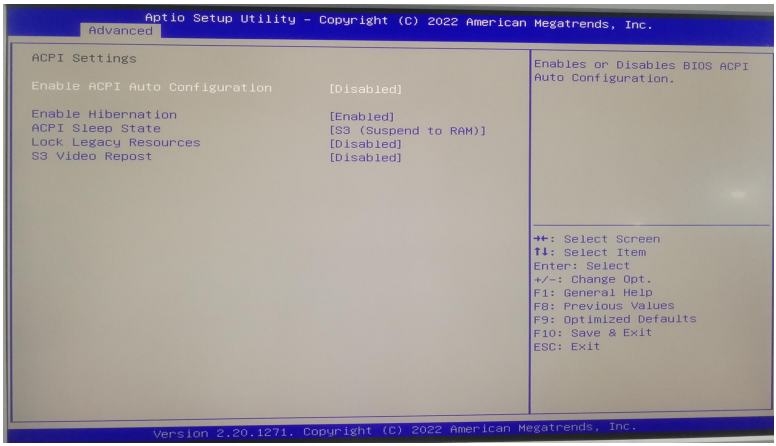
TPM2.0 UEFI Spec Version:选择支持的TCG规范版本，TCG_1_2兼容win8/10的模式，TCG_2 支持TCG2协议和时间格式，提供win10及以上的支持

Physical Presence Spec Version:选择上报给OS的支持PPI规范版本号,1.2支持PPI规范为1.2版本，1.3(默认)支持的PPI规范为1.3版本，一些HCK测试可能不支持1.3

TPM 20 InterfaceType:显示TPM2.0接口类型

Device Select:选择支持的TPM版本，TCM1.0,仅支持TCM1.0,TPM2.0仅支持TPM2.0,Auto(默认)同时支持TPM2.0和TCM1.0,若系统检测不到TPM2.0,则将枚举TCM1.0

3.2.8 ACPI Settings (ACPI 配置）



Enable ACPI Auto Configuration ： ACPI自动配置,默认Disabled。

Enable Hibernation ： 休眠设置。默认是关闭（Disabled）。这个选项在某些OS下不

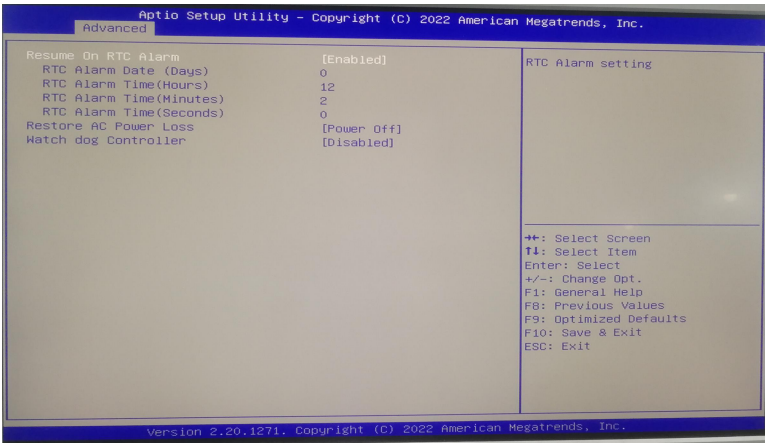
生效。

ACPI Sleep State ：选择系统睡眠时进入的省电模式，模式不一样，则系统功耗程度也不一样,Suspend Disabled;关闭休眠模式：S1(CPU Stop Clock)：CPU停止工作，其他设备仍然正常供电;S3(Suspend to Ram): 挂起到内存。

Lock Legacy Resources ：资源锁存，允许（Enabled）或关闭（Disabled）资源锁存功能。

S3 Video Repost：唤醒 S3/STR 睡眠模式的时候开启 VGA 的 BIOS POST 功能. 默认为Disabled。

3.2.9 Miscellaneous Configuration (杂项配置）



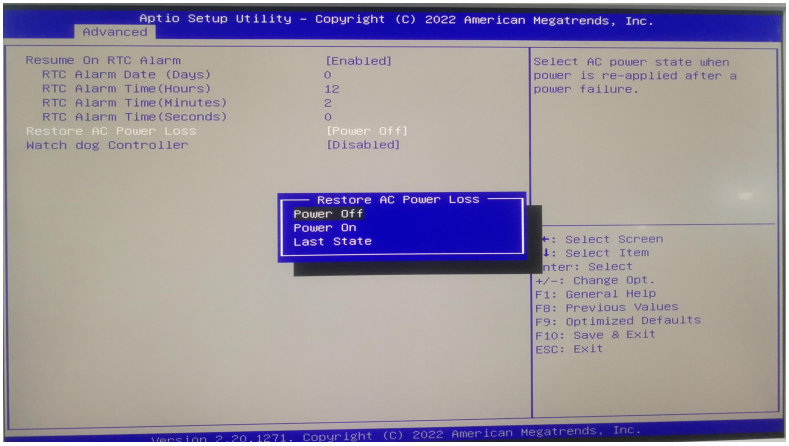
Resume On RTC Alarm :设置定时开机

RTC Alarm Date(Days):设置定时开机日期

RTC Alarm Time(Hours):设置定时开机小时

RTC Alarm Time(Minutes):设置定时开机分钟

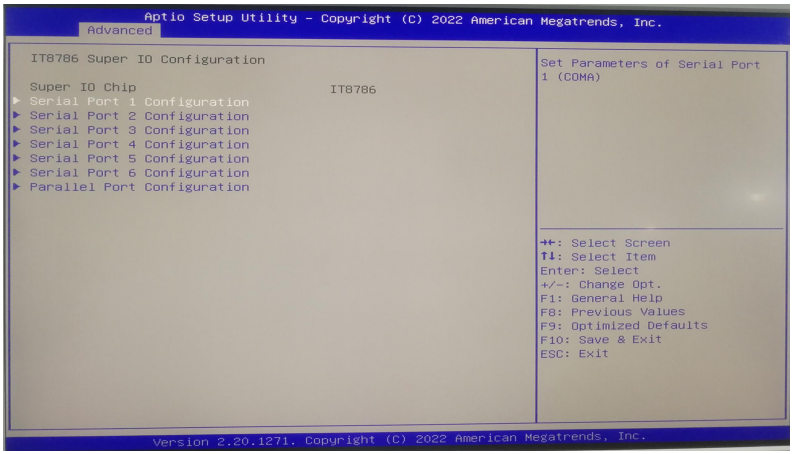
RTC Alarm Time(Seconds):设置定时开机秒



Restore AC Power loss:Power Off 当 AC 电源中断后系统进入关闭状态，Power On 当 AC 电源中断后系统维持启动状态，Last State 系统设置恢复到电源未中断之前的状态。

Watch dog Controller:设置看门狗，[Disabled]关闭看门狗，[Second mode]将看门狗设为秒的模式，[Minute Mode],将看门狗设为分钟的模式。

3.2.10 IT8786 Super IO Configuration (Super IO 配置）



Serial Port 1 Configuration：此项为串口1设置选项，Super IO 配置信息，包含COM 口中断号及地址设置。

Serial Port 2 Configuration：此项为串口2设置选项，Super IO 配置信息，包含COM 口

中断号及地址设置。

Serial Port 3 Configuration：此项为串口3设置选项，Super IO 配置信息，包含COM 口中断号及地址设置。

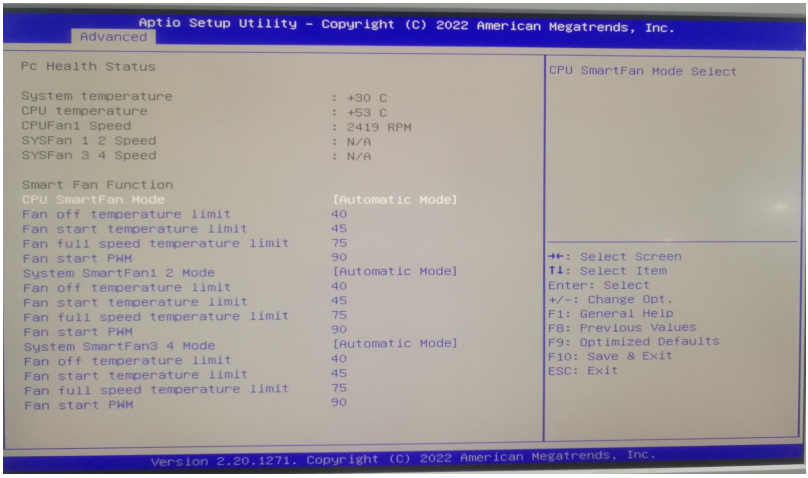
Serial Port 4 Configuration：此项为串口4设置选项，Super IO 配置信息，包含COM 口中断号及地址设置。

Serial Port 5 Configuration：此项为串口5设置选项，Super IO 配置信息，包含COM 口中断号及地址设置。

Serial Port 6 Configuration：此项为串口6设置选项，Super IO 配置信息，包含COM 口中断号及地址设置。

Parrallel Port Configuration:此项为并口设置选项，包含打印口中断号及地址设置。

3.2.11 Hardware Monitor (硬件侦测）



硬件侦测，显示当前系统温度，CPU温度，风扇转速，以及电压值。以上参数都有一定的范围，系统不可以超过这些范围运行。

CPU SmartFan Mode:是否开启CPU自动风扇控制功能，用于根据实时侦测的CPU温度来自动调整CPU风扇转速，从而达到省电节能的目的。

Fan off temperature limit:风扇关闭的最小温度值设置。

Fan start temperature limit:风扇开启的最小温度值设置。

Fan full speed temperature limit: 风扇全速运转的最小温度值设置

Fan start PWM:风扇的起始PWM的值设置。

System SmartFan1 2 Mode:是否开启系统自动风扇控制功能，用于根据实时侦测的系统温度来自动调整系统风扇转速，从而达到省电节能的目的。

Fan off temperature limit:风扇关闭的最小温度值设置。

Fan start temperature limit:风扇开启的最小温度值设置。

Fan start PWM:风扇的起始PWM的值设置。

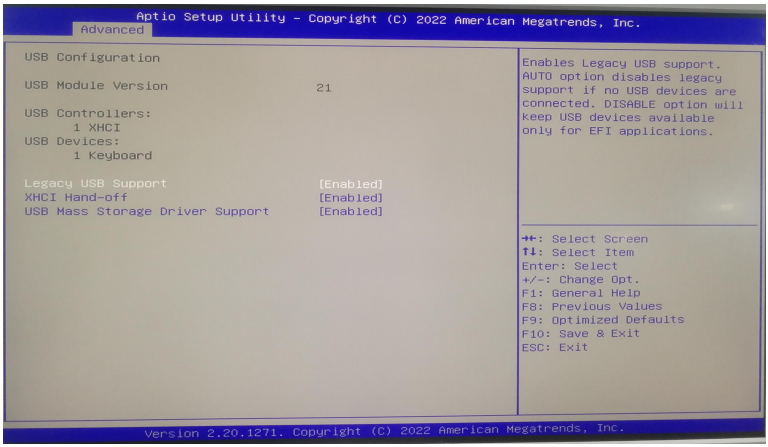
System SmartFan3 4 Mode:是否开启系统自动风扇控制功能，用于根据实时侦测的系统温度来自动调整系统风扇转速，从而达到省电节能的目的。

Fan off temperature limit:风扇关闭的最小温度值设置。

Fan start temperature limit:风扇开启的最小温度值设置。

Fan start PWM:风扇的起始PWM的值设置。

3.2.12 USB Configuration(USB 配置)

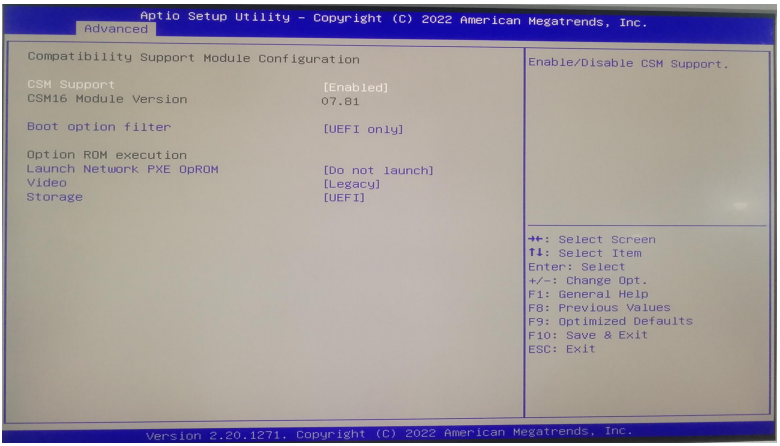


Legacy USB Support：[Enabled]启动在传统操作系统中支持USB设备功能，[Disabled]USB设备只能在BIOS程序设置中使用，无法在启动设备列表中背侦测到，[Auto]系统可以在开机时便自动侦测是否有USB设备存在，若是，则启动USB控制器。

XHCI Hand-off:可扩展主机控制器接口配置，适用于USB3.0，对于USB3.0 XHCI控制权的管理，Enabled默认，开启可扩展主机控制器接口功能，

USB Mass Storage Driver Support :支持大容量USB存储设备。

3.2.13 CSM Configuration(兼容性配置)

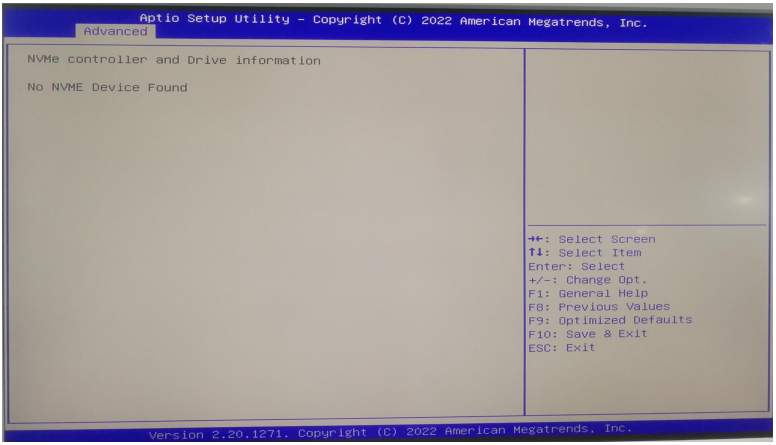


CSM Support：开启CSM以支持非UEFI驱动的附加设备

Boot option filter:LEGACY only,UEFI only,UEFI and LEGACY only,默认UEFI only

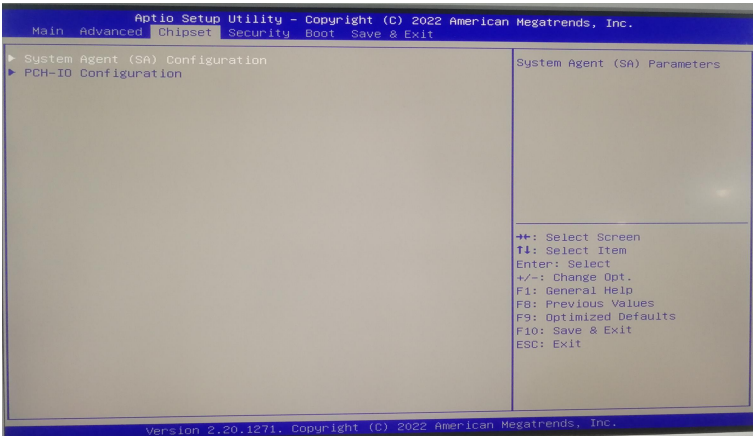
Launch Network PXE OpROM： 运行预启动执行环境兼容支持

3.2.14 NVME Configuration(NVME 配置)

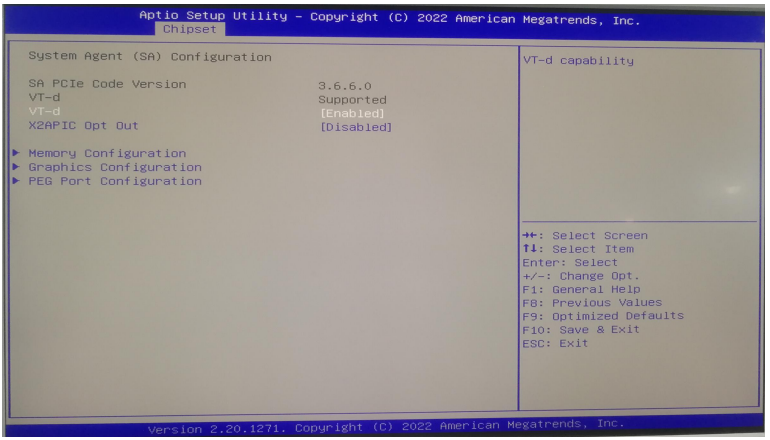


显示已链接设备的NVME控制器与驱动信息

3.2.15 Chipset 菜单(芯片组设置)



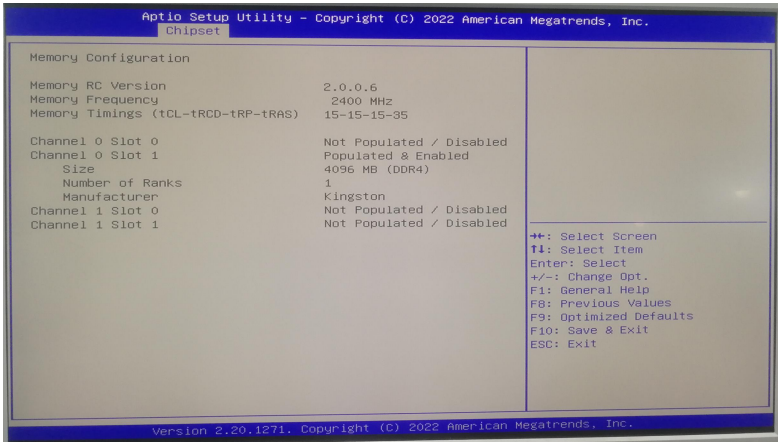
System Agent(SA) Configuration ： 系统代理设置



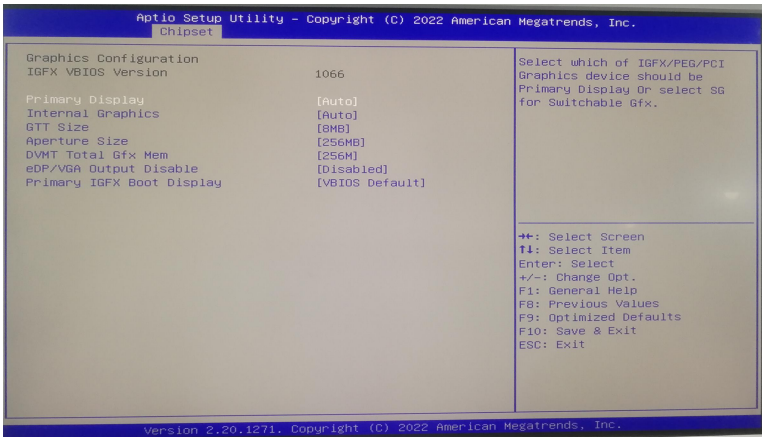
VT-d: 英特尔定向I/O虚拟化技术

X2APIC Opt out:支持扩展APIC，默认关闭，开启该选项后，会导致无法安装或者进入某些Linux 系统

Memory Configuration:设置内存参数



Graphics Configuration:用来选择处理器或PCIe显示设备作为优先使用的显示设备



Primary Display:选择以CPU、PCIE或PCI显示设备作为优先使用的显示设备

Internal Graphics:集成显示

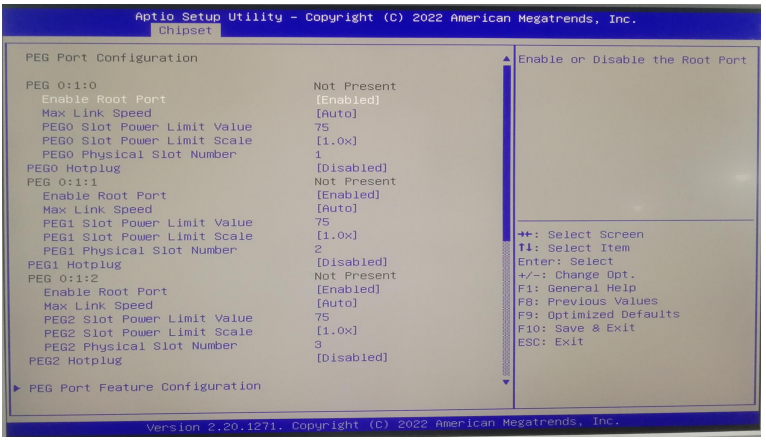
GTT Size:显存大小

Aperture Size：集成显卡显存调节

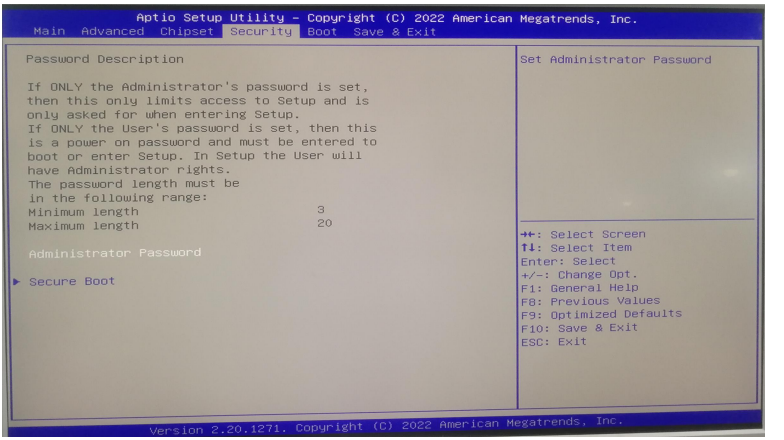
DVMT Total Gfx Mem：动态分配总的显卡的值

Primary IGFX Boot Display:设置主显示

PEG Port Configuration:PEG接口设置



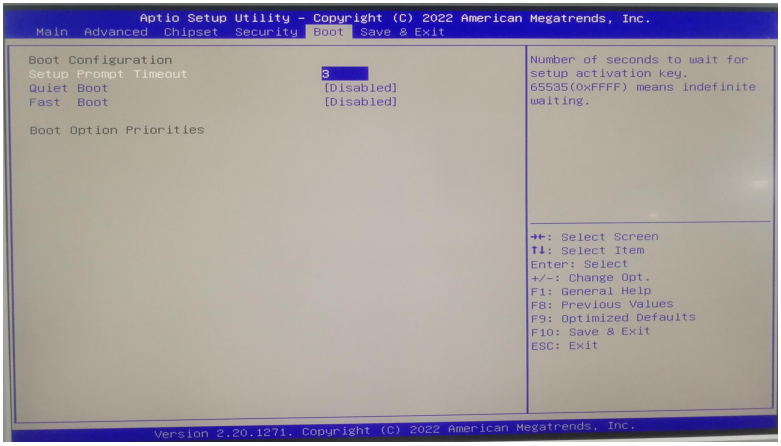
3.2.16 Security(安全设置)



密码字符长度提示：最小长度为3，最大长度为20。

Administrator Password ：该提示行用来设置超级用户密码。

3.2.17 BOOT(启动设置)



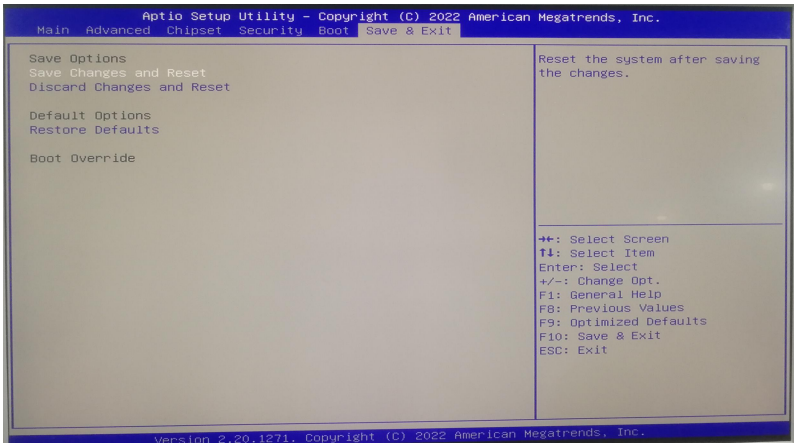
Setup Prompt **Timeout**：设置提示超时时间，按 Setup 快捷键的等待时间。如果在设置时间内没有按 Setup 快捷键就继续启动。

Quiet Boot：快速启动，可以设置计算机是否在启动时进行自检功能（POST）

Boot Option Priorities：系统将按照设定好的顺序来检测设备，直到找到一个能启动的设备，然后从这个设备启动。启动选项中**#1** 是最优先的启动设备。

Fast Boot ：快速启动（Disabled 关闭 ,enable 开启）。

3.2.14 Save & Exite(保存和退出)



Save Changes and Reset:保存 BIOS 设置并退出设置界面，继续启动计算机。

Discard Changes and Reset:放弃更改并退出设置界面，重启计算机。
Restore Defaults:载入优化设置，如果选择此项，系统将回复出厂的默认值进行设置
Boot Override ：选择指定 Boot 的设备，比如 SATA 硬盘，U 盘，EFI Shell，PXE 等，直接 Boot, 不用保存退出，按 F11 选择指定设备 Boot。

附录

附录一：术语表

ACPI

高级配置和电源管理。ACPI 规范允许操作系统控制计算机及其附加设备的大部分电能。

BIOS

基本输入/输出系统。是在 PC 中包含所有的输入/输出控制代码界面的软件。它在系统启动时进行硬件检测，开始操作系统的运作，在操作系统和硬件之间提供一个界面。BIOS 是存储在一个只读存储器芯片内。

BUS

总线。在计算机系统中，不同部件之间交换数据的通道，是一组硬件线路。我们所指的 BUS 通常是 CPU 和主内存元件内部的局部线路。

Chipset

芯片组。是为执行一个或多个相关功能而设计的集成芯片。我们指的是由南桥和北桥组成的系统级芯片组，他决定了主板的架构和主要功能。

CMOS

互补金属-氧化物半导体。是一种被广泛应用的半导体类型。它具有高速、低功耗的特点。我们指的 CMOS 是在主板上的 CMOS RAM 中预留的一部分空间，用来保存日期、时间、系统信息和系统参数设定信息等。

COM

串口。一种通用的串行通信接口，一般采用标准 DB9 公头接口连接方式。

DIMM

双列直插式内存模块。是一个带有内存芯片组的小电路板。提供 64bit 的内存总线宽度。

DRAM

动态随机存取存储器。是一个普通计算机的通用内存类型。通常用一个晶体管和一个电容来存储一个位。随着技术的发展，DRAM 的类型和规格已经在计算机应用中变得越来越多样化。例如现在常用的就有：SDRAM、DDR SDRAM 和 RDRAM。

LAN

局域网络接口。一个小区域内相互关联的计算机组成的一个计算机网络，一般是在一个企事业单位或一栋建筑物。局域网一般由服务器、工作站、一些通信链接组成，一个终端可以通过电线访问数据和设备的任何地方，许多用户可以共享昂贵的设备和资源。

LED

发光二极管，一种半导体设备，当电流流过时它会被点亮，通常用来把信息非常直观的表示出来，例如表示电源已经导通或硬盘驱动器正在工作等。

PnP

即插即用。允许 PC 对外接设备进行自动配置，不用用户手动操作系统就可以自己工

作的一种规格。为实现这个特点，BIOS 支持 PnP 和一个 PnP 扩展卡都是必需的。

POST

上电自检。在启动系统期间，BIOS 会对系统执行一个连续的检测操作，包括检测 RAM，键盘，硬盘驱动器等，看它们是否正确连接和是否正常工作。

PS/2

由 IBM 发展的一种键盘和鼠标连接的接口规范。PS/2 是一个仅有 6PIN 的 DIN 接口，也可以用以连接其他的设备，比如调制解调器。

USB

通用串行总线。一种适合低速外围设备的硬件接口，一般用来连接键盘、鼠标等。一台 PC 最多可以连接 127 个 USB 设备，提供一个 12Mbit/s 的传输带宽；USB 支持热插拔和多数据流功能，即在系统工作时可以插入 USB 设备，系统可以自动识别并让插入的设备正常。

附录二：常见故障分析与解决

常见故障	检查点
通电之后不开机	1. 请确认电源连接线是否连接正常 2. 请确认所用电源是否满足主板的供电要求 3. 尝试重新插拔内存条 4. 尝试更换内存条 5. 尝试根据主板说明书清除主板CMOS 6. 请确认是否有外接卡，去除外接卡后是否正常
开机后VGA不显示	1 查看显示器是否有打开 2 检查电源线是否正确地连接到显示器和系统单元 3 检查显示器电缆是否正确地连接到系统单元和显示器 4 查看显示屏亮度控件是否设置为黑暗状态,可通过亮度控件提高

	亮度。有关详细信息,可参考显示器操作说明 5 显示器处于“节电”模式,按键盘上的任意键即可
BIOS Setup设置不能保存	1. 请确认CMOS电池电压是否低于2.8V，如低于2.8V，请更换新电池，重新设置保存 2. BIOS设置不正确,根据开机画面提示的按键（DEL）,在 BIOS Setup 中调整时间和日期
提示无法找到可引导设备	1. 请确认硬盘电源线、数据线是否连接正常 2. 请确认硬盘是否有物理损坏 3. 请确认硬盘中是否正常安装操作系统
进入系统过程中蓝屏或死机	1. 请确认内存条及外接卡是否松动 2. 尝试去掉新安装的硬件，卸载驱动或软件 3. 尝试更换内存
进入操作系统缓慢	1. 尝试使用第三方软件检查硬盘是否有坏道 2. 请确认系统所在分区剩余空间是否过少 3. 请确认 CPU 散热风扇是否正常转动
系统自动重启	1. 请确认 CPU 散热风扇是否正常转动 2. 请确认是否误触发工控机复位按钮 3. 请使用杀毒软件确认系统是否感染病毒 4. 请确认内存条及外接卡是否松动 5. 请确认所用电源带载能力是否足够，可尝试更换电源
无法检测到USB设备	1. 请确认 USB 设备是否需要单独供电 2. 请确认 USB 接口是否存在接触不良 3. 请确认 BIOS Setup 中 USB 控制器是否打开