Mizar TTM2000 产品数据手册

版本 1.3　2022 年 6 月

上海芯钛信息科技有限公司

TTM2000 产品

Mizar TTM2000 是一款面向汽车电子领域的灵活、可靠、安全、合规的加密芯片产品。该产品针对车联网 V2X 应用安全进行了专门的开发设计，能够完全满足 C-V2X 和 DSRC 等应用场景所需的消息认证性能、安全证书管理等需求。

- 标准和认证
  - EVITA 硬件安全模块 Full 级架构设计
  - AEC-Q100 等级 1 级
  - EAL4+
  - 中国国家密码局安全芯片等级 2 级
- 产品特性
  - ARM® SecureCore® SC300™ 32-Bit RISC Core，80Mhz
  - 120.0DMIPS (Dhrystone v2.1)；
  - Memory Protection Unit (MPU)；
  - 24-bit SysTick 定时器；
  - 3.3V 和 1.8V 供电,IO 引脚电平为 3.3V
  - 工作温度范围：-40℃ - 125℃
  - 封装 LQFP-64
- 安全特性
  - 具有硬件“信任根”防篡改检测功能，物理屏蔽层防护设计，抗侧信道攻击防护设计
  - 内部集成国际标准和中国国家密码局标准的硬件密码算法单元
  - 4 路独立真随机数发生器
  - 硬件加密 Flash，密钥加密安全存储
  - 看门狗定时器(WDT)
  - 高/低电压异常检测
  - 温度异常检测
- 密码算法单元
  - 高速 ECDSA（NIST-P256）
  - 高速 SM2
  - 高速 SM3
  - RSA（up to 2048 bits）
  - ECC-256
  - SHA-256
  - AES
  - DES
  - SM4
- 系统保护
  - 每颗芯片均有 32 位唯一的序列号
  - 完善的生命周期状态管理

  - 使用国产密码算法的系统安全启动
- 通信特性
  - 2 个集成 SPI 控制器，仅配置为 Slave 模式
  - 1 个 UART 控制器
  - 1 个 I^2C
  - 5 通道 GPIO，3 路用于通讯标志使用；
  - 1 个外部定时器
  - 1 个 Watchdog
  - 8 通道 DMA 控制器
  - 多种类、可配置 IO 连接实现更优性能和灵活性
- 存储器
  - 512KB 内部 Flash，支持 ECC
  - 160KB SRAM
  - 安全 ROM

版本更新记录

版本日期	版本号	更改描述
2019 年 3 月	0.1	创建文件
2019 年 6 月	0.5	增加设计原理、封装信息等内容
2019 年 7 月	0.7	根据实际样品测试情况增加电气参数等内容
2019 年 10 月	0.9	FullMask LQFP64 封装芯片说明，修正原理图 PIN 5 标注
2019 年 12 月	0.91	单独列出了芯片功耗指标
2019 年 12 月	0.92	增加测试点建议和热阻信息
2019 年 12 月	0.93	增加硬件加速器性能参数和功率参数说明
2019 年 12 月	0.94	修正表 1 中的引脚定义
2020 年 1 月	0.95	增加 IO 引脚的电平参数
2020 年 1 月	0.96	增加 SPI 时序图
2020 年 3 月	0.97	增加订货信息和包装信息
2020 年 3 月	0.98	增加封装尺寸公差
2020 年 4 月	0.99	修正电气特性和热阻信息 修正硬件电路图中晶振要求
2020 年 7 月	1.0	增加了产品系列命名规则
2020 年 12 月	1.1	增加了 SPI 时序图和功能说明
2021 年 12 月	1.2	修正了文字排版、技术描述，增加了相关电路参考设计
2022 年 6 月	1.3	补充了 SPI 连接方式声明

目 录

1 系统框图

Mizar TTM2000 的内部架构图，请参考图 1.

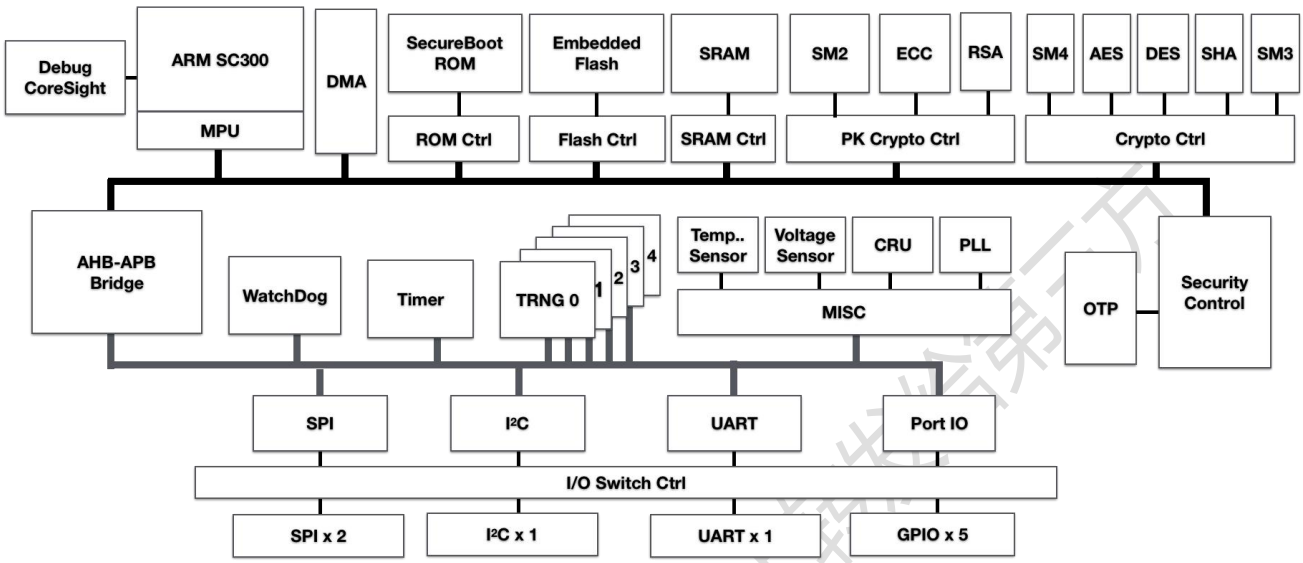


图 1. TTM2000 系统框图

2 功能简介

Mizar TTM2000 产品一款面向汽车电子领域的加密芯片产品，该产品按照 EVITA 定义的汽车 HSM 硬件架构设计，达到 EVITA 完整级 HSM 的硬件功能配置。产品集成了独立的安全专用处理器，并集成了国际标准的硬件密码算法 AES、SHA、DES、RSA、ECC 单元和中国国家密码局标准的硬件密码算法 SM2、SM3、SM4 单元；产品的生产封装制造等流程符合汽车级质量管控要求，产品达到了 AEC-Q100 Grade1 可靠性指标，并通过了由专业检测机构进行的完整的 AEC Q100 可靠性测试试验；产品整体安全性符合《GM/T0008 安全芯片密码检测准则》技术要求等级 2 级要求，并取得了国家密码产品资质认证。

TTM2000 产品可为网联汽车 V2X 应用所需的消息认证提供超高性能的硬件加速能力，同时作为安全芯片可提供关键秘密数据的存储，如私钥、根证书链等。整个应用框图，请参考图 2.

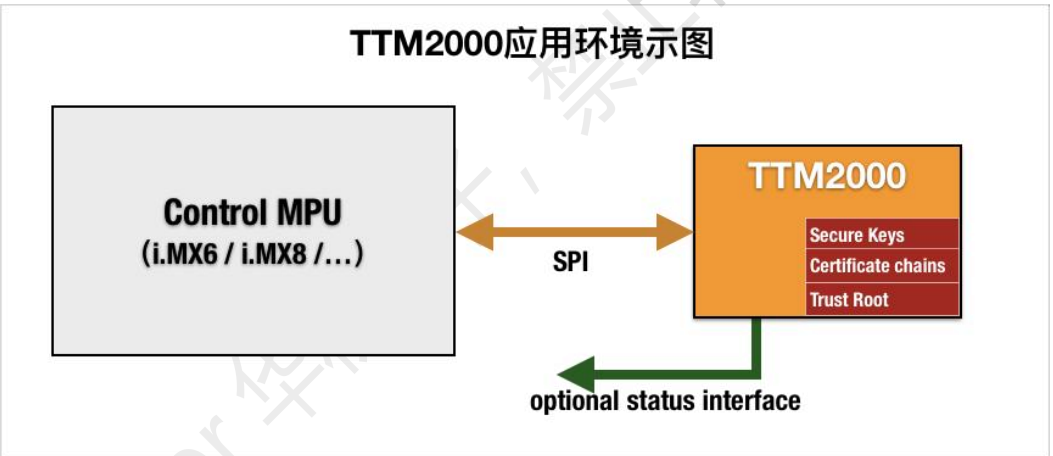


图 2. TTM2000 应用框图

Mizar TTM2000 提供 SPI 接口与上位机进行数据交互，上位机通过调用芯片接口可进行各类密码运算、密钥产生、密钥存储及管理、真随机数产生等操作，实现上位机应用需要的各类安全功能服务。

更多电路设计、加密功能接口等产品信息细节，请咨询芯钛的技术支持来获取 Mizar TTM2000 的产品资料及设计套件。

3 封装引脚

这章主要是描述了 TTM2000 的封装和引脚分配。

3.1 64-Pin LQFP

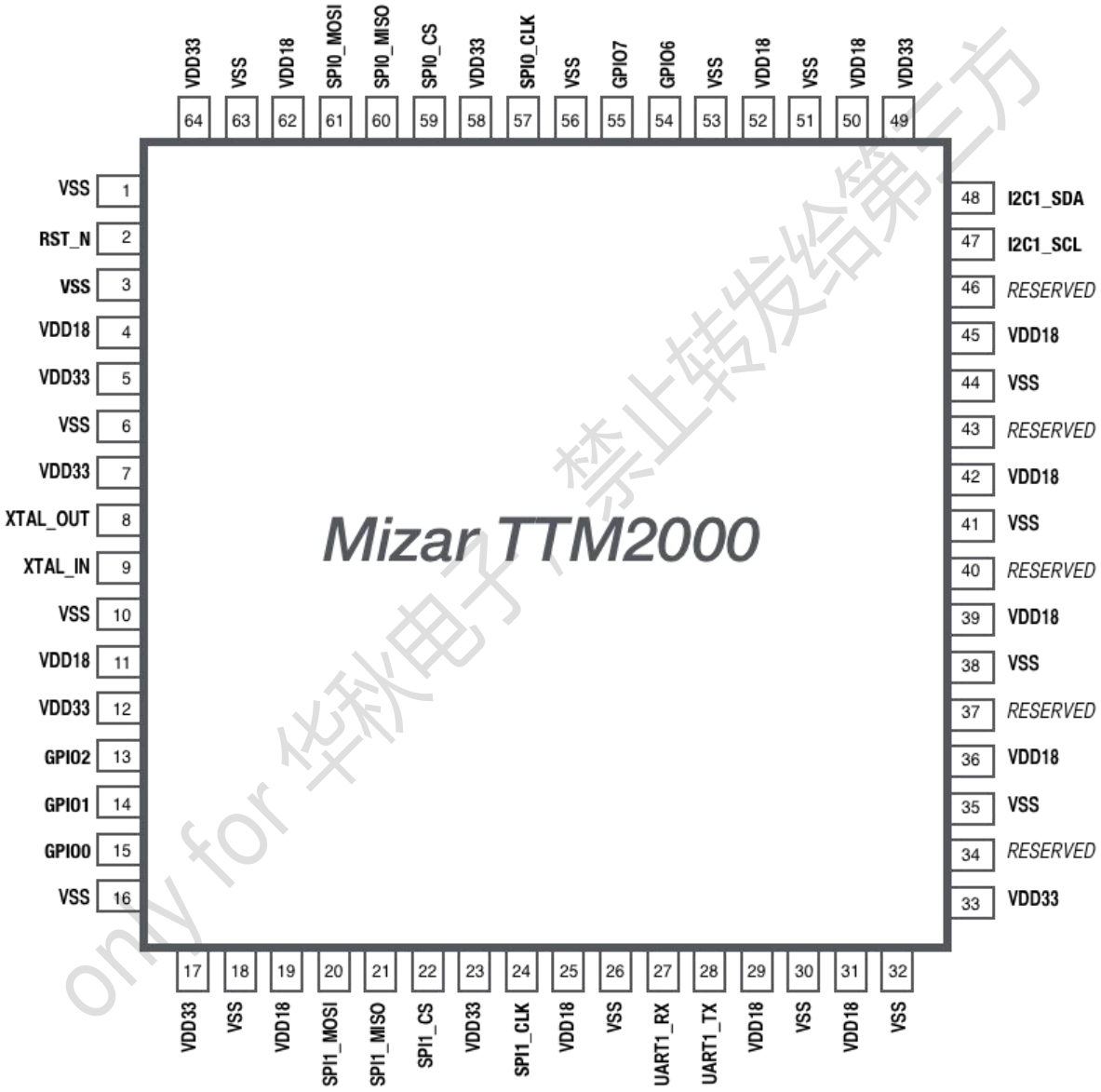


图 3. TTM2000 64 引脚 LQFP 封装

注：

所有的 VDD33 引脚均必须连到电源平面，建议使用 0.1uF 的去耦电容直连并靠近每一个 VDD33 引脚。所有的 VSS 引脚均必须连接到地平面。

3.2 引脚功能定义

引脚编号及其对应功能说明如下:

表 1. 引脚分配

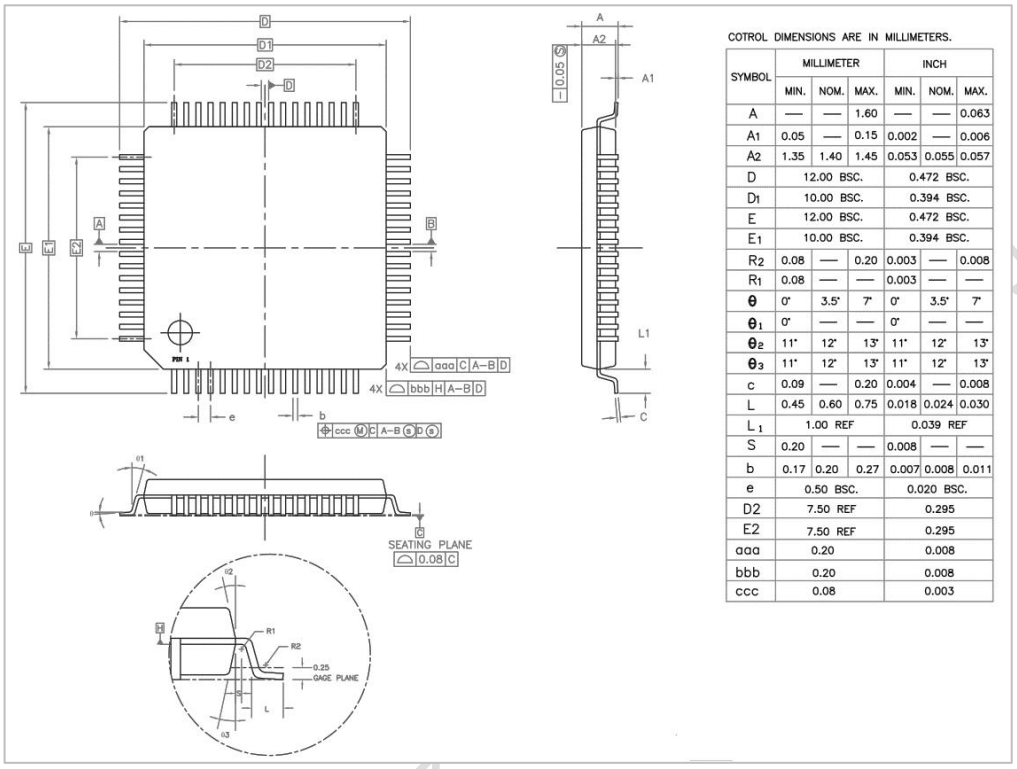
引脚号	引脚名称	引脚功能	电平类型	信号方向
1	VSS	地	0V	N/A
2	RST_N	复位信号，片内上拉	3.3V	输入
3	VSS	地	0V	N/A
4	VDD18	1.8V 电源	1.8V	N/A
5	VDD33	3.3V 电源	3.3V	N/A
6	VSS	地	0V	N/A
7	VDD33	3.3V 电源	3.3V	N/A
8	XTALOUT	晶振/振荡器输出	3.3V	模拟引脚
9	XTALIN	晶振/振荡器输入	3.3V	模拟引脚
10	VSS	地	0V	N/A
11	VDD18	1.8V 电源	1.8V	N/A
12	VDD33	3.3V 电源	3.3V	N/A
13	GPIO2	通用 IO2	3.3V	双向
14	GPIO1	通用 IO1	3.3V	双向
15	GPIO0	通用 IO0	3.3V	双向
16	VSS	地	0V	N/A
17	VDD33	3.3V 电源	3.3V	N/A
18	VSS	地	0V	N/A
19	VDD18	1.8V 电源	1.8V	N/A
20	SPI1_MOSI	SPI1 接口数据，可配置为主设备数据输出或从设备数据输入，片内下拉（从）（可 disable 下拉）	3.3V	双向
21	SPI1_MISO	SPI1 接口数据，可配置为主设备数据输入或从设备数据输出	3.3V	双向
22	SPI1_CS	SPI1 片选，可配置为主设备片选输出或从设备片选输入，片内上拉（从）（可 disable 上拉）	3.3V	双向
23	VDD33	3.3V 电源	3.3V	N/A
24	SPI1_CLK	SPI1 接口时钟，可配置为主设备或从设备，片内下拉（从）（可 disable 下拉）	3.3V	双向
25	VDD18	1.8V 电源	1.8V	N/A
26	VSS	地	0V	N/A
27	UART1_RX	UART 串行输入	3.3V	输入
28	UART1_TX	UART 串行输出	3.3V	输出
29	VDD18	1.8V 电源	1.8V	N/A
30	VSS	地	0V	N/A
31	VDD18	1.8V 电源	1.8V	N/A
32	VSS	地	0V	N/A
33	VDD33	3.3V 电源	3.3V	N/A
34	*NC*	*不连接*		*N/A*

35	VSS	地	0V	N/A
36	VDD18	1.8V 电源	1.8V	N/A
37	*NC*	*不连接*		*N/A*
38	*VSS*	*地*	0V	*N/A*
39	VDD18	1.8V 电源	1.8V	N/A
40	*NC*	*不连接*		*N/A*
41	VSS	地	0V	N/A
42	VDD18	1.8V 电源	1.8V	N/A
43	*NC*	*不连接*		*N/A*
44	VSS	地	0V	N/A
45	VDD18	1.8V 电源	1.8V	N/A
46	*NC*	*不连接*		*N/A*
47	I2C1_SCL	I2C1 接口时钟，可配置为主设备或从设备，片内上拉（可 disable 上拉）	3.3V	双向
48	I2C1_SDA	I2C1 接口数据，可配置为主设备或从设备，片内上拉（可 disable 上拉）	3.3V	双向
49	VDD33	3.3V 电源	3.3V	N/A
50	VDD18	1.8V 电源	1.8V	N/A
51	VSS	地	0V	N/A
52	VDD18	1.8V 电源	1.8V	N/A
53	VSS	地	0V	N/A
54	GPIO6	通用 IO6	3.3V	输出
55	GPIO7	通用 IO7	3.3V	输出
56	VSS	地	0V	N/A
57	SPI0_CLK	SPI0 接口时钟，可配置为主设备或从设备，片内下拉（从）（可 disable 下拉）	3.3V	双向
58	VDD33	3.3V 电源	3.3V	N/A
59	SPI0_CS	SPI0 片选，可配置为主设备片选输出或从设备片选输入，片内上拉（从）（可 disable 上拉）	3.3V	双向
60	SPI0_MISO	SPI0 接口数据，可配置为主设备数据输入或从设备数据输出	3.3V	双向
61	SPI0_MOSI	SPI0 接口数据，可配置为主设备数据输出或从设备数据输入，片内下拉（从）（可 disable 下拉）	3.3V	双向
62	VDD18	1.8V 电源	1.8V	N/A
63	VSS	地	0V	N/A
64	VDD33	3.3V 电源	3.3V	N/A

注：SPI 不支持一主多从的连接方式

3.3 封装尺寸说明

TTM2000 支持 LQFP-64 封装，引脚间距 0.5mm。MSL 等级为 3 级。图 1 是机械尺寸图，图 2 是 PCB 建库尺寸参考图。



COTROL DIMENSIONS ARE IN MILLIMETERS.

SYMBOL	MILLIMETER			INCH		
	MIN.	NOM.	MAX.	MIN.	NOM.	MAX.
A	—	—	1.60	—	—	0.063
A1	0.05	—	0.15	0.002	—	0.006
A2	1.35	1.40	1.45	0.053	0.055	0.057
D	12.00 BSC.			0.472 BSC.		
D1	10.00 BSC.			0.394 BSC.		
E	12.00 BSC.			0.472 BSC.		
E1	10.00 BSC.			0.394 BSC.		
R2	0.08	—	0.20	0.003	—	0.008
R1	0.08	—	—	0.003	—	—
θ	0°	3.5°	7°	0°	3.5°	7°
θ1	0°	—	—	0°	—	—
θ2	11°	12°	13°	11°	12°	13°
θ3	11°	12°	13°	11°	12°	13°
c	0.09	—	0.20	0.004	—	0.008
L	0.45	0.60	0.75	0.018	0.024	0.030
L1	1.00 REF			0.039 REF		
S	0.20	—	—	0.008	—	—
b	0.17	0.20	0.27	0.007	0.008	0.011
e	0.50 BSC.			0.020 BSC.		
D2	7.50 REF			0.295		
E2	7.50 REF			0.295		
aaa	0.20			0.008		
bbb	0.20			0.008		
ccc	0.08			0.003		

参数	最小值	典型值	最大值	单位
D1, E1	9.8	10	10.2	mm
D, E	11.8	12	12.2	mm

图 4. 封装机械图（含公差）

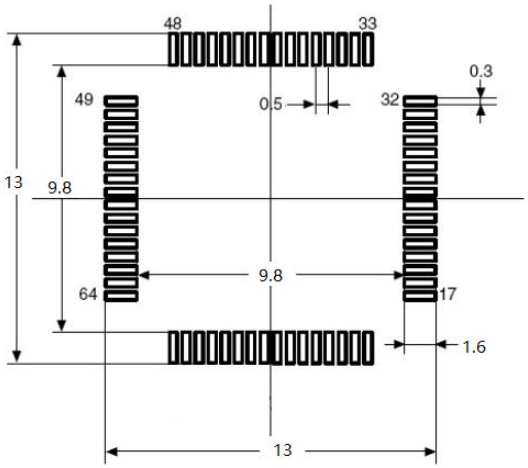


图 5. PCB 建库尺寸参考图

4 电气特性

4.1 极限条件

表 2. 极限条件

类别	参数含义	条件	最小值	最大值	单位
VDD33	3.3V 电源电压	所有 VDD33 管脚	-0.3	5.8	V
VDD18	1.8V 电源电压	所有 VDD18 管脚	-0.3	2.4	V
VI	信号输入电压	所有输入管脚	-0.3	5.8	V
I_{SS}	工作地管脚电流	所有 VSS 管脚	-	250	mA
T_{stg}	存储温度	非供电	-55	150	℃
T_{amb}	环境温度	工作状态	-40	125	℃
I_{lat}	栓锁电流	信号管脚	-	100	mA
V_{ESD}	抗静电	HBM，所有管脚	-	2000	V
	抗静电	CDM，所有管脚	-	500	V

4.2 工作条件

Mizar TTM2000 工作环境温度-40℃~125℃，芯片工作时的典型电气特性如下：

表 3. 典型电气特性

类别	参数含义	条件	最小值	典型值	最大值	单位
VDD33	3.3V 电源电压	所有 VDD33 管脚	2.7	3.3	3.6	V
VDD18	1.8V 电源电压	所有 VDD18 管脚	1.62	1.8	1.98	V
I_{DD33}	VDD33 工作电流	VDD33=3.3V	10	15	20	mA
I_{DD1V8} *1	VDD18 工作电流	VDD18=1.8V	20	130	260	mA
I_{IL}	输入低电流	VI=0V，非上下拉管脚	-2	0	2	μA
I_{IH}	输入高电流	VI=3.3V，非上下拉管脚	-2	0	2	μA
V_{IH}	高输入门限电平	VDD33=3.3V	2.4	-	-	V
V_{IL}	低输入门限电平	VDD33=3.3V	-	-	0.8	V
V_{OH}	高输出门限电平	输出电流 6mA VDD33=3.3V	2.8	-	-	V
V_{OL}	低输出门限电平	输出电流 6mA VDD33=3.3V	-	-	0.4	V
R_{pullup}	片内上拉电阻		20	50	100	KOhm
$R_{pulldown}$	片内下拉电阻		20	50	100	KOhm
C_{in}	输入电容		-	-	10	pF

注：

1. VDD18 工作电流最大值的测量条件为通过 I/O 接口调用芯片的峰值运算状态（4500 次/秒 SM2 签名验证运算）。

4.3 功耗指标

表 4. 功耗指标

类别	最小值	典型值	最大值	单位
工作功耗*1	40	285	540	mW
热阻系数*2	--	48	--	°C/W

注：

1. 以上均为芯片实测结果。
2. 基于 LQFP64 封装的 JA 热阻。

4.4 硬件加速器性能

表 5. 算法性能

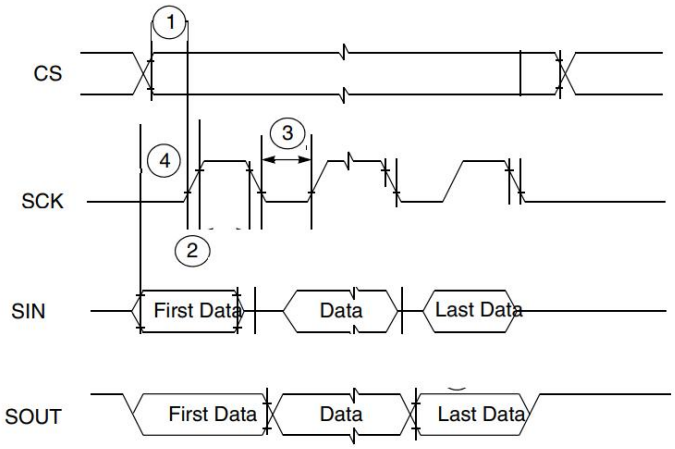
算法	测试通道	签名次数	验签次数	单位
SM2	内部	12500	7300	次/秒
ECC-NIST		12500	7300	次/秒
SM2	SPI (单通道)	3600	3400	次/秒
ECC-NIST		3500	3200	次/秒

注：以上为芯片实测数据。详细性能测试数据可参见芯钛公司提供的性能测试报告。

4.5 SPI 时序图

表 6. 时序参数

类别	最小值	典型值	最大值	单位
Tcsc	--	16.7	--	us
Trsi	--	24	--	ns
Tsdc	--	55	--	ns
Tsui	--	28	--	ns



5 IO 设备

5.1 GPIO 设备

Mizar TTM2000 包含一个 GPIO 接口设备，支持 5 路 GPIO PIN。

GPIO 模块具有如下特性：

- 兼容 AMBA APB2.0 总线；
- 支持 2 个单独可编程 GPIO PIN；
- 每个端口的方向可控制；
- PIN 在复位时默认为输入；
- 读写操作时，可通过地址线进行位屏蔽操作；
- 可编程控制中断；
- 上电复位期间，接口复位所有寄存器；
- 具有标识寄存器。

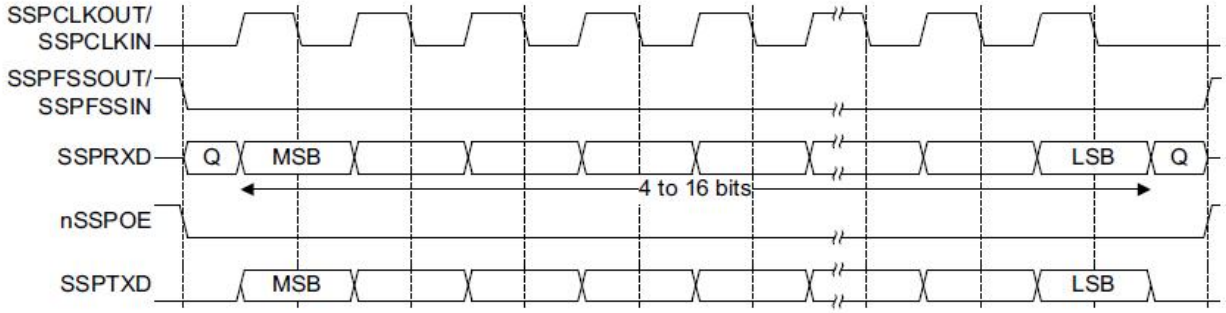
5.2 SPI 设备

SPI 接口设备是 Mizar TTM2000 与上位机通信的主要接口，其中包含 2 个 SPI 接口设备，与上位机建立通信链路，SPI 接口设备可工作在 DMA 模式或者中断模式。

SPI 模块具有如下特性：

- 最高支持 40MHz 传输速率
- 仅选择作为从机；
- 支持 SPI mode 01，全双工操作；
- 32 帧独立收发 FIFO；
- 支持每帧配置长度为 4～16 位；
- 支持 5 种中断类型；
- 通信辅助：SPI 需要和 GPIO 配对使用，配对规则是 SPI0 对应 GPIO6，SPI1 对应 GPIO7。

SPO=0，SPH=1 数据传输



5.3 I2C 设备

MIZAR TTM2000 包含 1 路 I2C 接口设备，也可以用来与上位机通信。与 SPI 接口相比 I2C 的速率相对较低，与上位机传输协议的设计上必须考虑大的延迟情况。

I2C 模块具有如下特性:

- 传输速度支持标准模式(0 至 100 KB/s)、快速模式(≤400 KB/s)
- 时间同步技术；
- I2C 主机/从机操作；
- 7 位或 10 位寻址；
- 7 位或 10 位组合格式传输；
- 批量传输模式
- 忽略 CBUS 地址
- 具有发送和接收缓冲区
- 中断或者轮询模式操作
- 可编程 SDA 保持时间(tHD; DAT)
- 可配置软件驱动程序支持的组件参数
- 通信辅助：I2C 需要和 GPIO 配对使用，配对规则是 I2C 对应 GPIO0。芯片的 I2C 地址： 0x5D

5.4 UART 设备

Mizar TTM2000 包含 1 路 16550 兼容的 UART 设备，用做调试端口，输出调试信息。

UART 模块具有如下特性:

- 分离 32 具有传输和 32 和有如接收 FIFO 内存缓冲区，以减少 CPU 中断；
- 禁用 1 字节深度的可编程 FIFO；
- 可编程波特率发生器，可以使用频率> 3.6864MHz 的任何时钟作为参考时钟；
- 标准异步通信位（启动、停止和奇偶校验）；
- 7 位或 10 位组合格式传输；
- 传输 FIFO、接收 FIFO、接收超时、调制解调器状态和错误状态中断的独立屏蔽；
- 支持 DMA；
- 错误启动位检测
- 断线产生和检测
- 支持调制解调器控制功能 CTS、DCD、DSR、RTS、DTR 和 RI
- 可编程硬件流控制
- 全可编程串行接口特性
    - 数据可以是 5、6、7 或 8 位
    - 偶数、奇数或无奇偶校验位生成和检测
    - -1 或 2 停止位生成
    - 波特率生成，DC 最高为 UARTLK/16
- 唯一标识 UART 的标识寄存器

6 参考电路

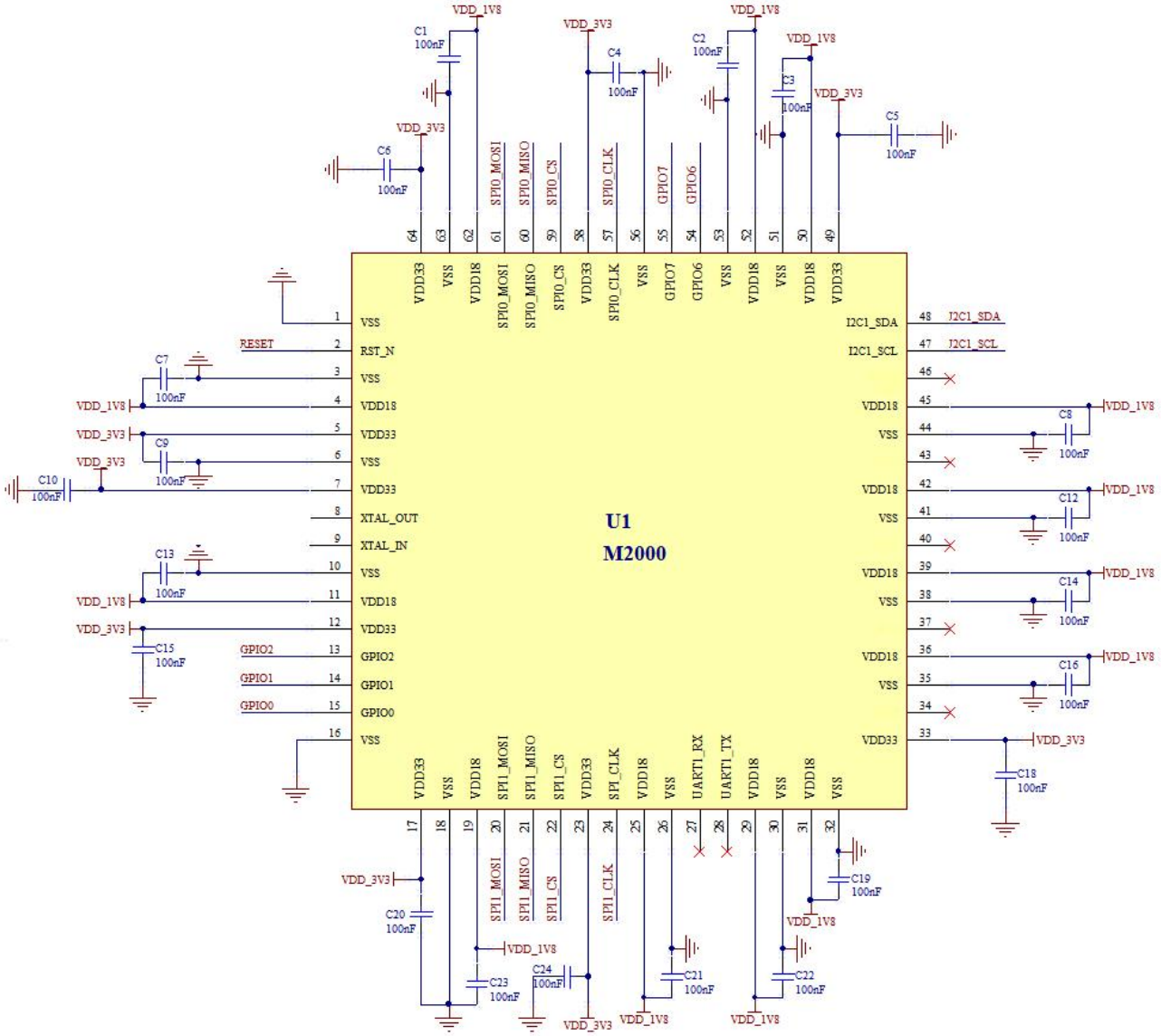


图 6. TTM2000 参考电路图

注：

1. 时钟只能使用 16MHz 无源晶振，2%精度，晶振电路参考设计如下图所示：

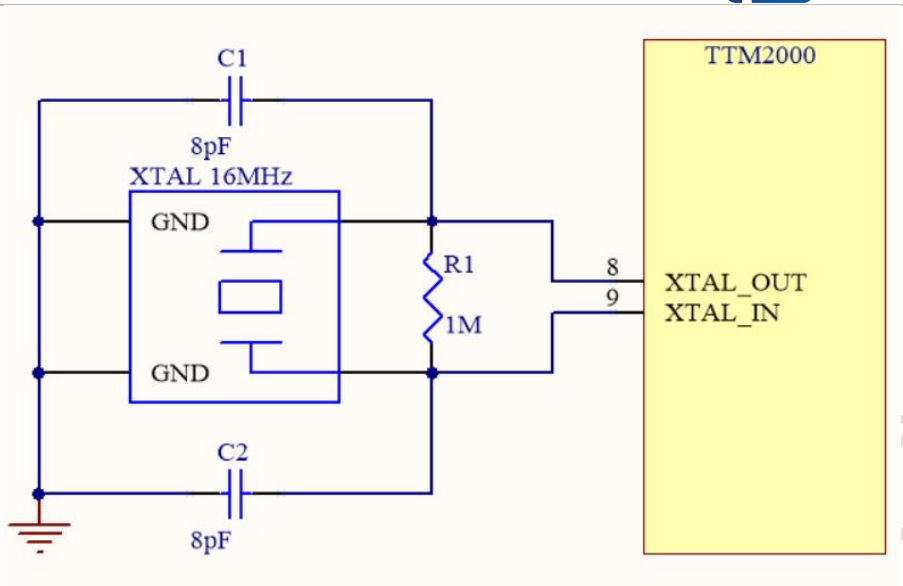


图 7. 晶振电路参考设计

2. 复位信号低电平有效，复位时将 Pin 2（RESET）拉低 100 微秒以上再释放即完成复位动作。复位电路参考设计如下图所示：

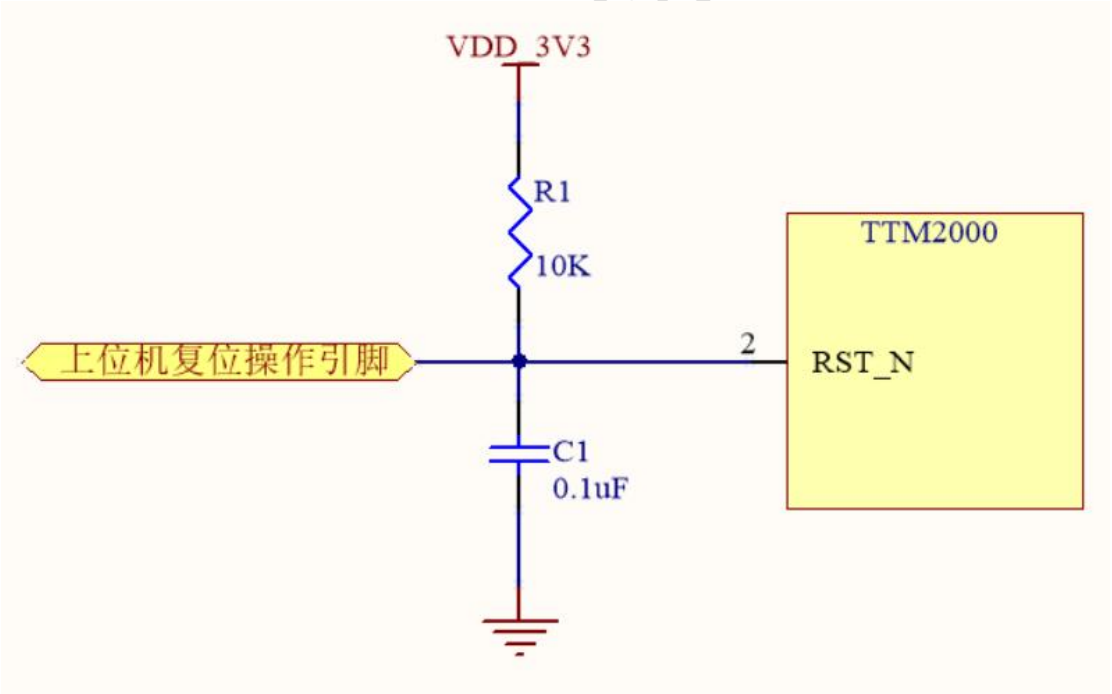


图 8. 复位电路参考设计

3. 如果需要将多个上位机的复位操作引脚连接到 TTM2000 的复位引脚时，建议通过逻辑门电路互联，参考设计如下图所示；其中任何一个上位机执行复位操作都会导致 TTM2000 与其他上位机正在执行的业务出现异常。

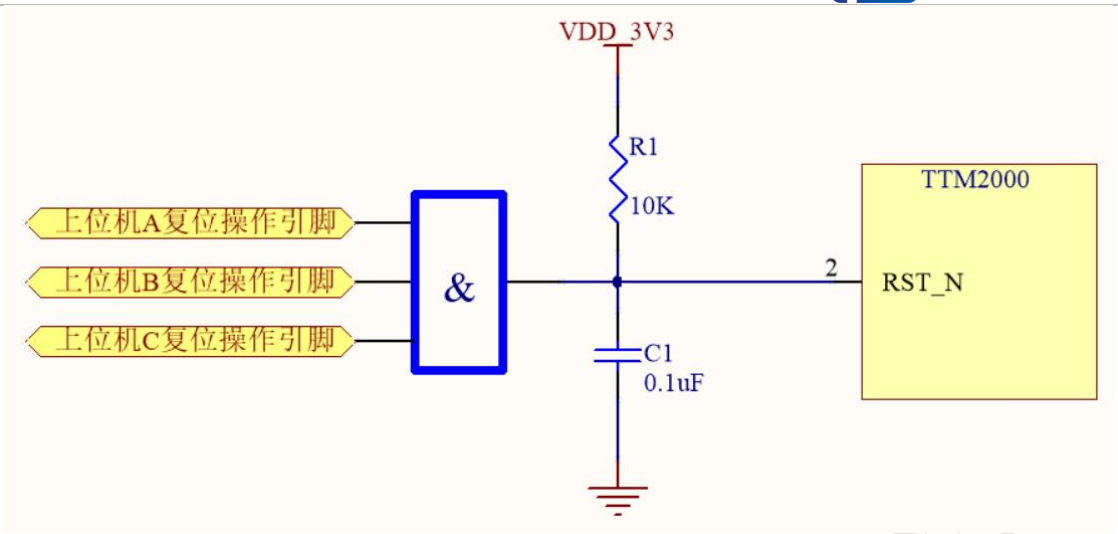


图 9. 多上位机复位操作引脚连接参考设计

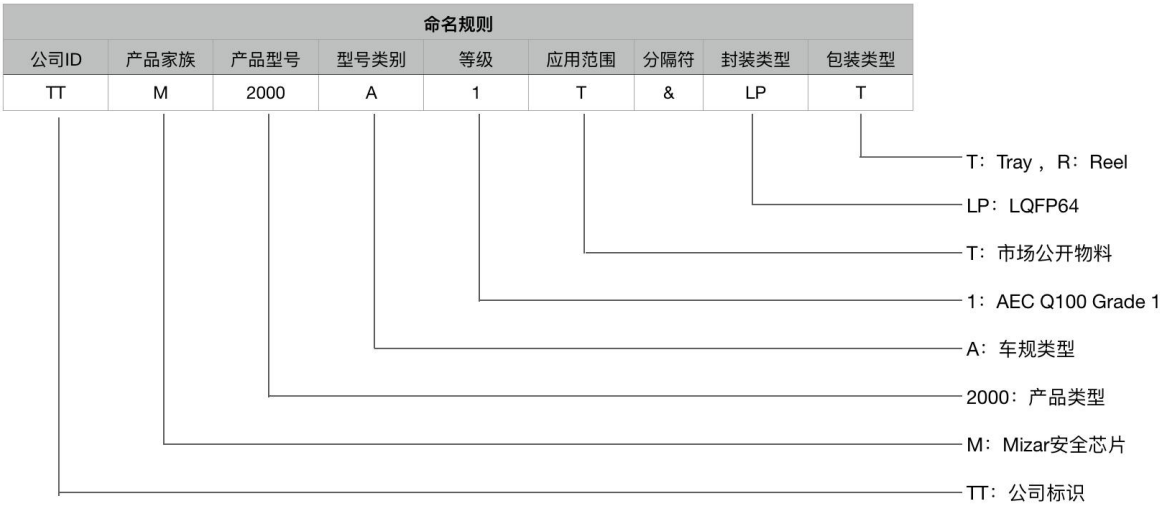
4. 芯片上电时序，VDD3V3 先于 VDD1V8 0~100 微秒上电。
5. 上电复位过程中，上位机应保持 PIN54(GPIO6)和 PIN55(GPIO7)这两个引脚为低电平。
6. 针对项目需求，Mizar TTM2000 与上位机通信需要使用 GPIO PIN 辅助，SPI 设备使用 PIN54(GPIO6)和 PIN55(GPIO7)两个引脚，I2C 设备使用 PIN15（GPIO0）引脚。PIN27(UART1_RX)，PIN28(UART1_TX), PIN54(GPIO6)和 PIN55(GPIO7)等 4 个引脚建议保留测试点，具体信息请联系芯钛技术支持获取项目详细信息。
7. SPI 不支持一主多从的连接方式。

7 订货信息

Mizar TTM2000 订货信息如下表。

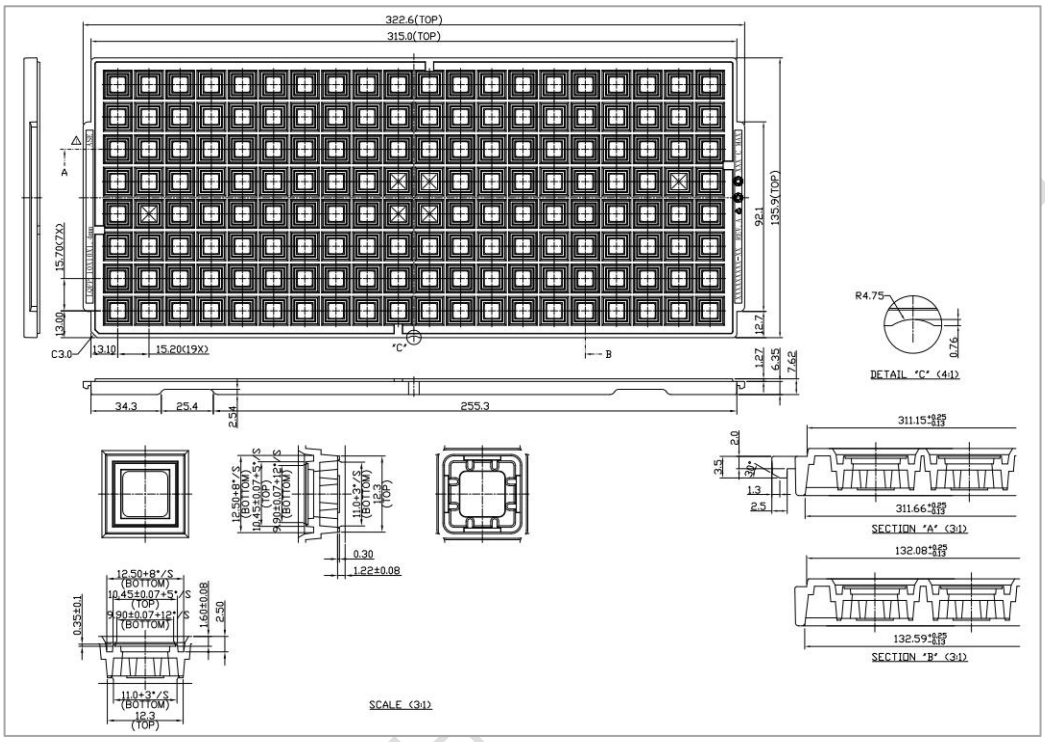
表 7. 订货信息

封装	封装形式	单位数量	最小订货量	ROHS
LQFP-64	托盘	160	320	是
LQFP-64	卷带	1500	1500	是



8 包装信息

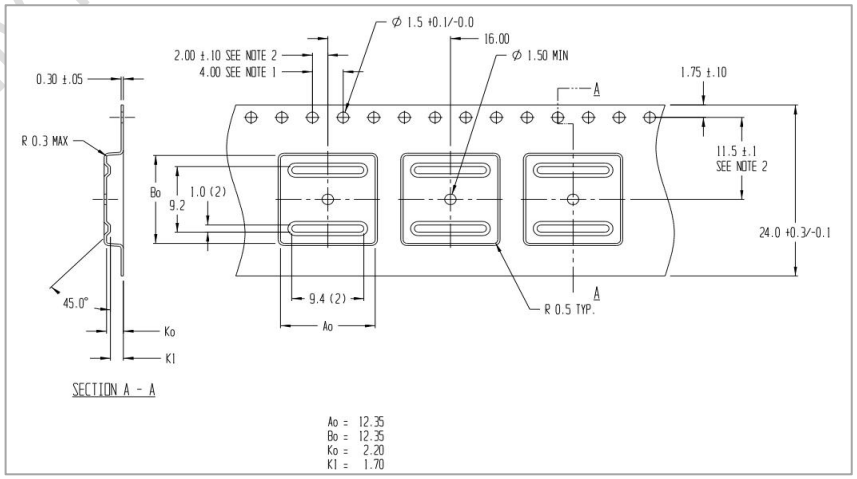
8.1 托盘包装图



注：

1. 表面电阻率≥1.0×105 & ＜1.00×1^{12}ohm/sq；
2. 翘曲控制在 0.76mm 以内；
3. 可用单元为 8×20 = 160 个；

8.2 卷带包装图



声明

芯钛认为本文档中的信息是准确可靠的，保留随时更改信息和规格的权利，本文档取代并替代了先前版本中提供的所有信息。

联系信息

更多信息，请联系 support@thinktech.net.cn