



SQ7101/SQ7103

简要中文产品规格书 V2.1

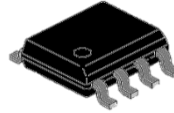
No. : TDDS01-S7101-CN(B)	Name : SQ7101/SQ7103 简要中文产品规格书	Version : V2.1
--------------------------	--------------------------------	----------------

SQ7101/SQ7103 , Secure ASIC, AES-128/AES-256, SHA-256, TRNG

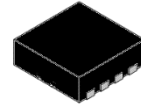
◆ 基本信息:

- 工作电压范围: 2.0V ~ 5.5V
- 工作温度范围: -40°C ~ 85°C

封装形式:



SOP8



8-Lead DFN
(3mm x 3mm)

◆ 低功耗平台

- 低功耗设计支持运作(operation)与深眠(Deep Sleep)模式
- 深眠模式功耗 250nA

◆ 通讯接口

- SQ7101 持I2C界面(Max: 400KHz)
- SQ7103 支持SPI界面(Max: 5MHz@MODE0)

◆ 安全加密防护功能:

- AES-128/AES-256 硬件加解密算法
- SHA-256 硬件哈希算法
- 真随机数生成器(true random number generator, TRNG)
- 物理上使用强力密封和防篡改电路, 提高密钥和敏感数据保护能力
- 差分功耗分析旁路攻击保护(SPA/DPA : simple/differential power analysis)
- 独立的内部时钟、可防止外部Glitch攻击
- 128位唯一识别码 (UID)
- NIST CAVP Certification

◆ 应用项目:

- 配件认证、耗材认证
- 系统反仿冒
- 加密电子锁、指纹锁
- 对话密钥交换 (Session Key Exchange)
- 连网装置安全识别或认证
- 敏感数据加密
- 上位机软件、版权保护
- 嵌入式系统固件(Firmware)保护
- 安全链路、安全控制

◆ 支持16个128-bit 或8个256-bit 密钥

◆ 256 Bytes 用户数据(User Data)

◆ 768 Bytes Small Zone

◆ 内建 16个monotonic 计数器、防止replay 攻击及中间人(man in the middle)攻击

目录

1. 产品简介	5
1.1 重点说明	5
2. 引脚配置	6
2.1 SQ7101 引脚配置/说明	6
2.2 SQ7103 引脚配置/说明	8
3. 电气特性	11
3.1 极限参数	11
3.2 工作条件	11
3.2.1 工作条件	11
3.2.2 I/O 特性	11
3.3 DC 特性	12
3.4 上电复位电气特性	12
3.5 BROR 电气特性	14
3.6 AC 特性	14
3.6.1 运行模式时序特性	14
3.6.2 I2C 特性	16
3.6.3 SPI 特性	17
3.7 EEPROM 特性	19
附录 A. 封装信息	20
修改记录	23

1. 产品简介

1.1 重点说明

SQ7101/SQ7103 为一高安全性、低功耗之加密芯片，支持 16 个 128-bit 或 8 个 256-bit 密钥，具有真随机数生成器，以硬件实现 AES-128/AES-256 加密运算法、SHA-256 哈希算法，具备差分功耗分析旁路攻击保护功能大幅提升加密安全性。具标准 I2C(SQ7101)以及 SPI(SQ7103)通信接口，易于整合到原有的设计中，进行产品安全升级。

SQ7101/SQ7103 加密芯片适用于配件/耗材认证、系统反仿冒、加密电子锁、指纹锁、对话密钥交换 (Session Key Exchange)、连网装置安全识别或认证、敏感数据加密、...等高安全性的应用需求。

2. 引脚配置

2.1 SQ7101 引脚配置/说明

产品型号: SQ7101SP008C00R

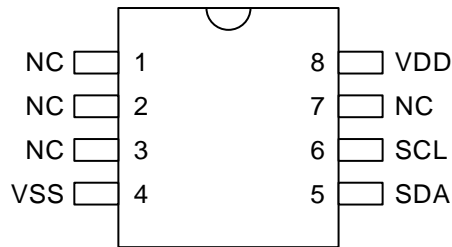


图 2-1 SQ7101 SOP8 封装型态引脚配置

产品型号: SQ7101N3008C00R

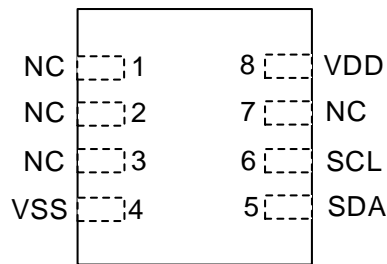


图 2-2 SQ7101 8-Lead DFN 封装型态引脚配置

引脚编号	引脚名称与端口/选择功能	输入输出I/O类型	
1	NC	-	不连接
2	NC	-	不连接
3	NC	-	不连接
4	VSS	GND	接地
5	SDA	I/O	I2C总线, 串行数据输入/输出引脚
6	SCL	I	I2C总线, 串行时钟输入引脚
7	NC	-	不连接
8	VDD	电源	VDD电源输入

汉芝电子股份有限公司

iMQ Technology Inc.

No. : TDDS01-S7101-CN(B)	Name : SQ7101/SQ7103 简要中文产品规格书	Version : V2.1
--------------------------	--------------------------------	----------------

2.2 SQ7103 引脚配置/说明

产品型号: SQ7103SP008S00R

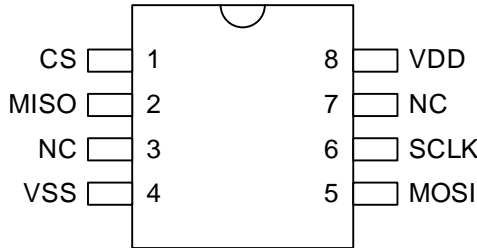


图 2-3 SQ7103 SOP8 封装型态引脚配置

产品型号: SQ7103N3008S00R

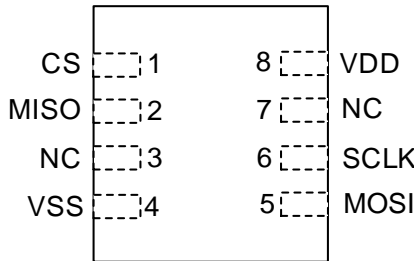


图 2-4 SQ7103 8L-DFN 封装型态引脚配置

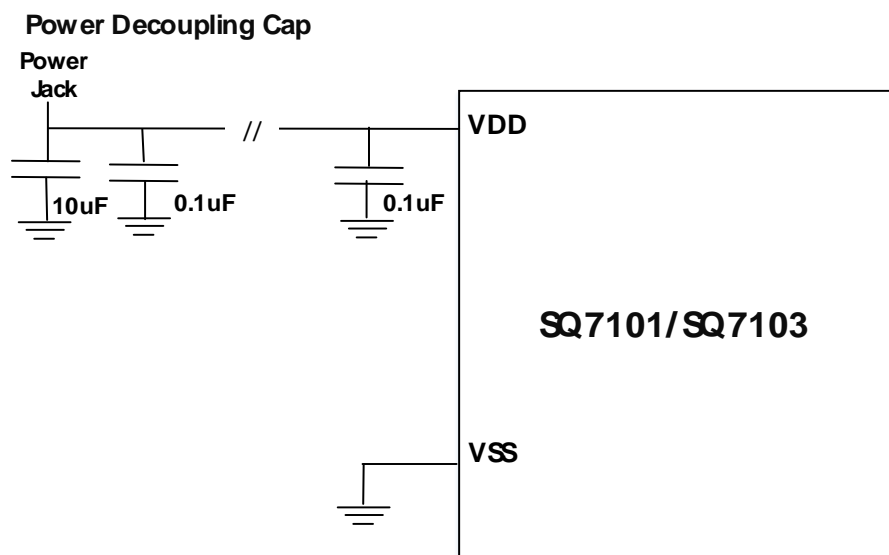
引脚编号	引脚名称与端口/选择功能	输入输出I/O类型	
1	CS	I	SPI,芯片选择引脚
2	MISO	O	主设备输入/从设备输出引脚
3	NC	-	不连接
4	VSS	GND	接地
5	MOSI	I	SPI,主设备输出/从设备输入引脚
6	SCLK	I	SPI,串行时钟输入引脚
7	NC	-	不连接
8	VDD	电源	VDD电源输入

汉芝电子股份有限公司

iMQ Technology Inc.

No. : TDDS01-S7101-CN(B)	Name : SQ7101/SQ7103 简要中文产品规格书	Version : V2.1
--------------------------	--------------------------------	----------------

以下为在使用 SQ7101/SQ7103 产品时建议的外部参考线路，若使用到相关引脚功能时，请参考所对应的接线建议：



注：上图近 IC 端 (VDD) 的 0.1uF，应该尽可能靠近 IC

No. : TDDS01-S7101-CN(B)	Name : SQ7101/SQ7103 简要中文产品规格书	Version : V2.1
--------------------------	--------------------------------	----------------

3. 电气特性

3.1 极限参数

加密芯片操作时切勿超过以下任一项极限参数值。即使仅是极短时间，也可能造成加密芯片损坏或性能衰退，严重者可能导致起火或爆炸、造成伤害。因此，请确保采用本加密芯片设计开发之产品或系统不超过以下极限参数值。

(V_{SS} = 0V)

参数	符号	引脚	极限参数	单位
供电电压范围	V _{DD}		-0.3 to 6.0	V
输入电压范围	V _{IN}	全部 I/O 引脚	-0.3 to VDD+0.3V	V
最大输出电流	I _{OL}	全部 I/O 引脚	50	mA
保存温度范围	T _{STG}		-50 to 125	°C

3.2 工作条件

以下定义出当装置于「电压及温度最大/最小值」运行时其电气特性。「标准」条件是在「室温 25°C 及标准工作电压 VDD=3.3V」下测定而得。

若有不同于以上定义或是更详细的工作条件，会于各表格中的「测试条件」字段中注明该条件。

3.2.1 工作条件

参数	符号	测试条件	最小	标准	最大	单位
工作电压	V _{DD}		2.0	3.3	5.5	V
工作温度	T _a		-40	25	85	°C

3.2.2 I/O 特性

参数	符号	测试条件	最小	标准	最大	单位
低电压输入	V _{IL}		0		0.3 VDD	V
高电压输入	V _{IH}		0.7 VDD		VDD	V
端口引脚之低电压输出	V _{OL}	IOL= 3 mA	0		0.1VDD	V
端口引脚之高电压输出	V _{OH}	IOH= -3 mA	0.9VDD		VDD	V

3.3 DC 特性

参数	符号	测试条件	最小	标准	最大	单位
运作模式 (Operation)	I _{DD_N1}	VDD=3.3V, Temp=25 °C		3		mA
深眠模式 (Deep Sleep)	I _{DD_DS}	VDD=3.3V, Temp=25 °C		250		nA

3.4 上电复位电气特性

Ta=-40~85°C					
符号	叙述	最小	标准	最大	单位
tPPW	上电复位最小脉宽 Power-on reset minimum pulse width	1	-	-	ms
tPWUP	上电复位后到装置 ready 时间 Warming-up time after a reset is clear and device ready	-	4	-	ms
tVDD	上电时间 Power supply rise time	0.5		5	ms

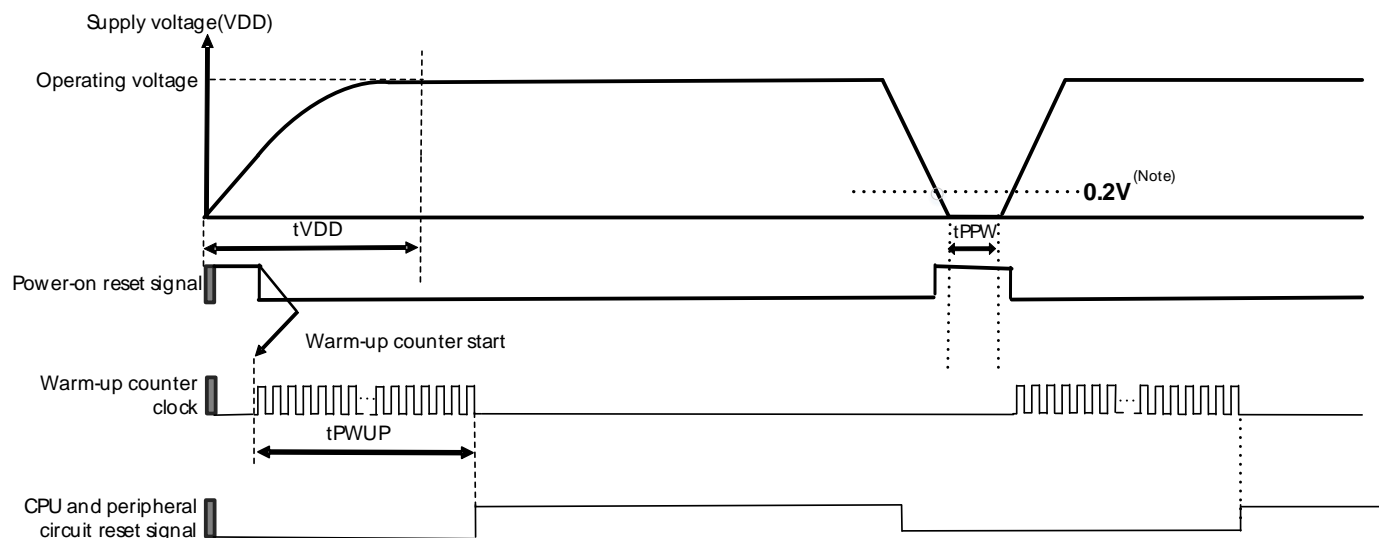


图 3-1 上电复位时序图

Note : 当系统下电时，电压需低到 0.2V 以下再重新上电，才能确保重新上电后的 IC 动作正常。

No. : TDDS01-S7101-CN(B)	Name : SQ7101/SQ7103 简要中文产品规格书	Version : V2.1
--------------------------	--------------------------------	----------------

3.5 BROR 电气特性

Ta=-40~85°C						
参数	符号	测试条件	最小	标准	最大	单位
BROR 检测电压	VBROR_Rising	VDD 上升时间和下降时间(rise time and fall time)> tVDD (tVDD 请参考 <u>Ch3.4 上电复位电气特性</u>)	1.95	2.0	2.05	V
	VBROR_Falling		1.85	1.90	1.95	V

3.6 AC 特性

参数	符号	最小	标准	最大	单位
用户数据更新时间 (User Data Write) (注)	T _{wc1}	6.0	-	9.0	mS
128-bit/256-bit 密钥更新时间 (Key Write Time) (注)	T _{wc2}	6.0		9.0	mS

注: Write time 包含数据更新以及自动检验之运作

3.6.1 运行模式时序特性

参数	符号	最小	标准	最大	单位
上電後就緒時間 Power-Up Ready Time	T _{PU_RDY}		2800	9300	uS
Standby 時間 · 進入 deep sleep 模式 Standby Time, Entering the deep sleep mode	T _{STB}		55	90	uS
喚醒就緒時間 · deep sleep 模式 Wake-Up Ready Time, deep sleep mode	T _{WDS_RDY}		300	-	uS

注：标准值为室温25°C之参考值，Sleep指令会改变此值。

汉芝电子股份有限公司

iMQ Technology Inc.

No. : TDDS01-S7101-CN(B)	Name : SQ7101/SQ7103 简要中文产品规格书	Version : V2.1
--------------------------	--------------------------------	----------------

3.6.2 I2C 特性

参数	符号	最小	最大	单位
SCL 时钟频率 (clock frequency)	f_{SCL}	0	400	kHz
重启条件保持时间 (hold time repeated START condition) 第一个时钟脉冲产生跟随在此时间之后发生。	$t_{HD;STA}$	0.6	-	us
SCL 时钟低电平周期 (low period of SCL clock)	t_{LOW}	1.3	-	us
SCL 时钟高电平周期 (high period of SCL clock)	t_{HIGH}	0.6	-	us
重启条件设置时间 (setup time for a repeated START condition)	$t_{SU;STA}$	0.6	-	us
数据保持时间 (data hold time)	$t_{HD;DAT}$	0	0.8	us
数据设置时间 (data setup time)	$t_{SU;DAT}$	0.1	-	us
SDA 与 SCL 上升时间 (rise time of both SDA and SCL)	t_r	20	300	ns
SDA 与 SCL 下降时间 (fall time of both SDA and SCL)	t_f	20	300	ns
停止条件设置时间 (setup time of STOP condition)	$t_{SU;STO}$	0.6	-	us
停止条件与开始条件间的总线自由时间 (bus free time between a STOP and START condition)	t_{BUF}	1.3	-	us
每条总线之电容负载(capacitive load for each bus line)	C_b	-	400	pF
注 1 : 以上为特性值, 非经生产测试。				

表 3-1 I2C AC 规格

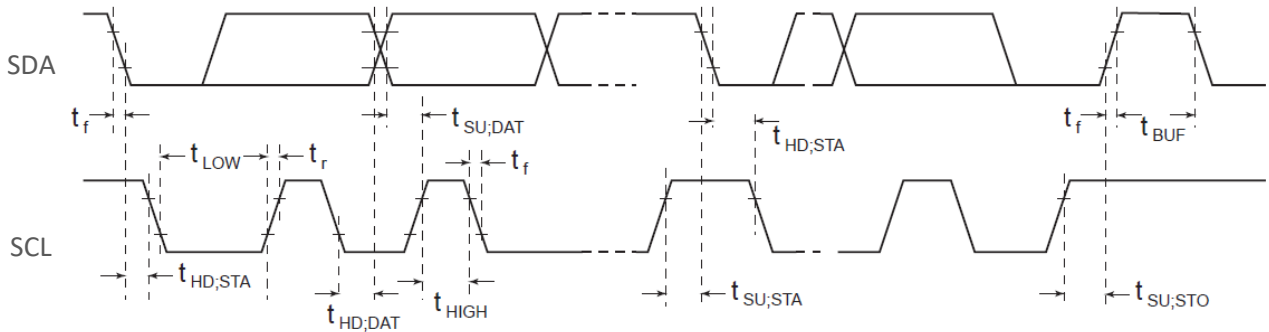


图 3-2 I2C 时序图

3.6.3 SPI 特性

参数	符号	最小	最大	单位
SPI 频率 (SPI Frequency)	f_{SPI}		5	MHz
SPI 周期 (SPI Period)	t_{SPI}	200		ns
SCLK 高电平周期 (High period of the SCLK pin)	t_{CLKH}	90		ns
SCLK 低电平周期 (Low period of the SCLK pin)	t_{CLKL}	90		ns
从 SPICS 有效到第一个边沿的时间 (From SPICS active to first edge)	t_{CS_SU}	40		ns
从最后一个 SCLK 边沿到 SPICS 无效的时间 (From last SCLK edge to SPICS inactive)	t_{CS_HD}	40		ns
SPI 传输时间 (Time between SPI transaction)	t_{CS_WA}	1		us
输入数据设置时间 (Data Input Setup Time)	t_{SI_SU}	10		ns
输入数据保持时间 (Data Input Hold time)	t_{SI_HD}	10		ns
输出数据有效时间 (Data Output Valid Time)	t_{SO_VD}		80	ns
输出数据保持时间 (Data Output Hold Time)	t_{SO_HD}	0		ns

表 3-2 SPI AC 规格

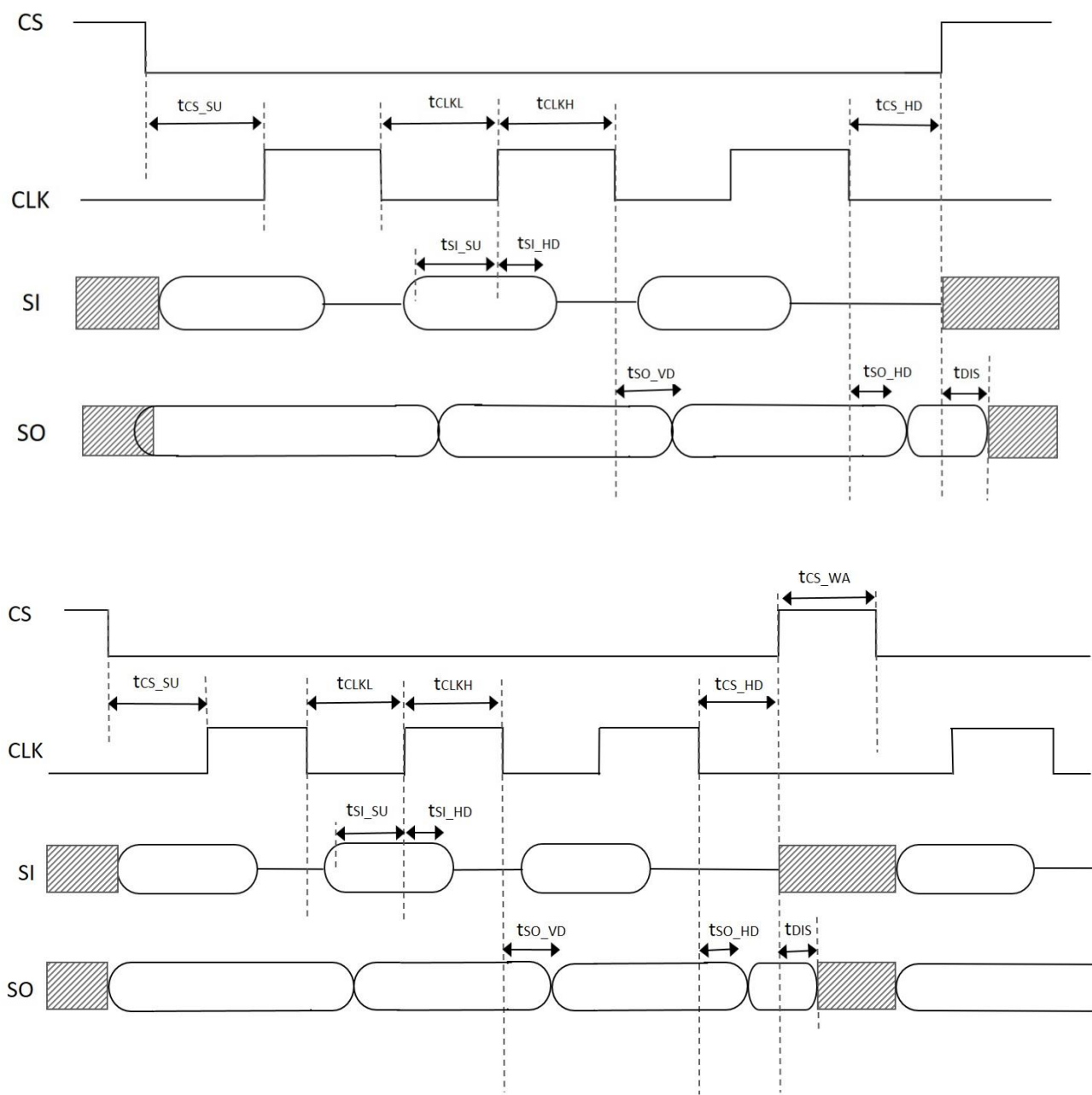


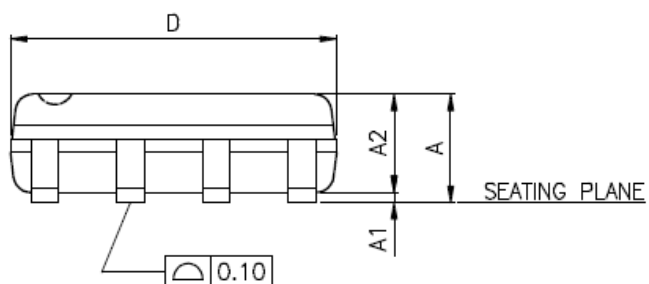
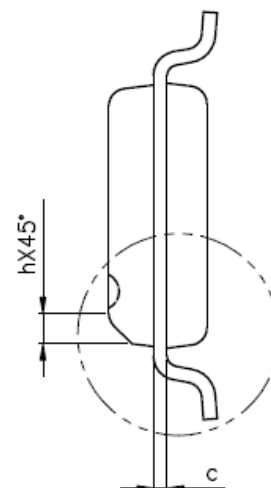
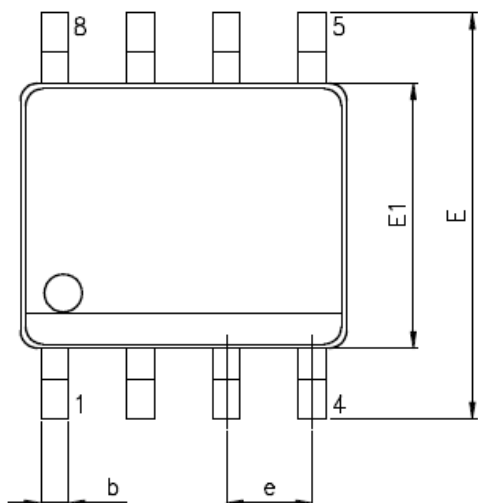
图 3-3 SPI 时序图

3.7 EEPROM 特性

参数	最小	标准	最大	单位
擦写次数(Write Endurance (Sector Endurance))	100,000	-	-	Cycles
数据保存期限(Data Retention(at 25°C))	100	-	-	Years
数据保存期限(Data Retention(at 85°C))	20	-	-	Years

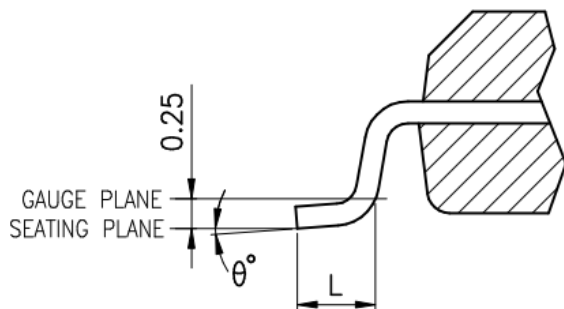
附录 A. 封装信息

SOP8

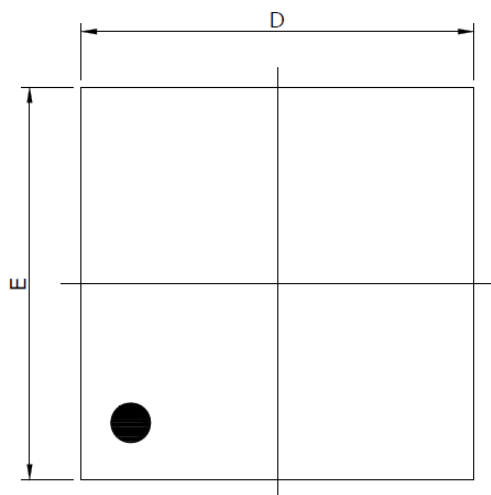


標號	毫米		
	最小值		最大值
A	--	--	1.75
A1	0.10	--	0.25
A2	1.25	--	--
b	0.31	--	0.51
c	0.10	--	0.25
D	4.90 BSC		
E	6.00 BSC		
E1	3.90 BSC		
e	1.27 BSC		
L	0.40	--	1.27
h	0.25	--	0.50
θ	0°	--	8°

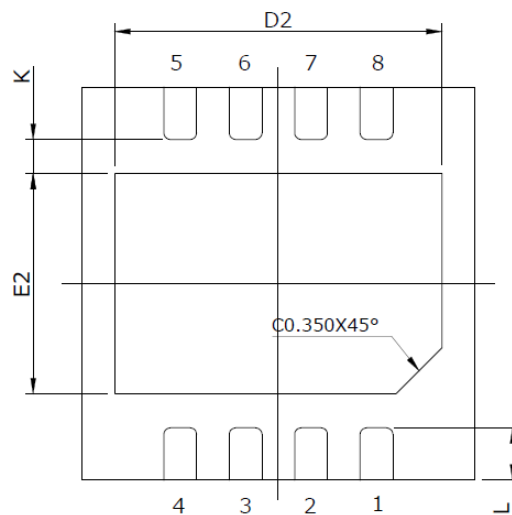
No. : TDDS01-S7101-CN(B)	Name : SQ7101/SQ7103 简要中文产品规格书	Version : V2.1
--------------------------	--------------------------------	----------------



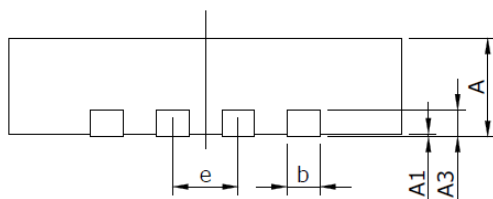
8L DFN (3mm x 3mm)



TOP VIEW



BOTTOM VIEW



標號	毫米		
	最小值		最大值
A	0.70	0.75	0.80
A1	0.00	0.02	0.05
A3	0.203 REF.		
b	0.20	0.25	0.30
D	2.90	3.00	3.10
E	2.90	3.00	3.10
e	0.50 BSC		
L	0.35	0.40	0.45
D2	2.45	2.50	2.55
E2	1.63	1.68	1.73
K	0.20	--	--

修改记录

版本	发布日期	改版描述
V2.1		1. 与完整版 V2.1 同步 2. 修订 3.1 极限参数 "工作电压"成为"供电电压"
V2.0	2024/03/4	3. 与完整版 V2.0 同步
V1.9	2023/12/26	4. 与完整版 V1.9 同步 5. 增订 SQ7103 8-Lead DFN 封装型态引脚配置 6. 增订产品型号: SQ7101SP008C00R, SQ7101N3008C00R, SQ7103SP008S00R, SQ7103N3008S00R
V1.7	2023/4/20	7. 修正工作电压范围 2.0~5.5V ; 修正"3.1 极限参数"与" 3.2.1 工作条件"的工作电压范围 8. 更新图 3-1 上电复位时序图与注"当系统下电时, 电压需低到 0.2 V 再重新上电, 才能确保重新上电后的 IC 动作正常" 9. "3.6.1 运行模式时序特性", 新增注1: "上电后就绪时间不包含BOOTROM code 执行时间; BOOTROM code 执行时间约需10ms。 10. "3.6.2 I2C特性" 新增 $t_{HD;DAT}$ 数值 11. 图 3-2 I2C 时序图, 新增 SDA,SCL 标示
V1.6	2022/11/3	1. 修正「3.4 上电复位电气特性」图 3-1 上电复位时序图与其备注
V1.5	2022/7/21	1. 「Small Zone 修改为 768 Bytes」 2. 「2.1 SQ7101 引脚配置/说明」与「附录 A 封装信息」新增 8L DFN 3x3
V1.4	2021/12/29	1. 修改 「上电复位时序图」 2. 新增 「CH3.5. BROR 电气特性」
V1.3	2021/11/30	1. 调整章节顺序 2. 新增 「CH3.4.上电复位电气特性」
V1.2	2021/6/24	1. 新增 「CH3.7. EEPROM 特性」说明。」
V1.1	2020/12/30	1. 新增 SQ7103 机种相关叙述、「CH2.2 SQ7103 引脚配置/说明」、「CH3.6.3 SPI 特性」
V1.0	2020/9/1	1. 首次发行