团　　体　　标　　准

T/XXXX-2021

面向燃气物联网 NB-IoT 智能表的安全芯片检测技术规范

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

*******发布**

目　　次

前　　言

为规范燃气物联网NB-IoT智能表安全芯片检测工艺的技术规范，制定本标准。

本标准按照T/CGAS 1000-2021《中国城市燃气协会标准起草规则》的规定起草。

本标准的主要内容：范围、规范性引用文件、术语和定义、符号和缩略语、对安全芯片的总体要求、安全芯片物理检测、安全芯片通信协议检测、安全芯片功能检测、安全芯片性能检测、安全芯片安全性检测、安全芯片可靠性检测、安全芯片兼容性和一致性检测、安全芯片检测条件与检测工具要求、附录。

本标准由中国城市燃气协会标准工作委员会归口。

本标准负责起草单位：北京市燃气集团有限责任公司。

本标准参加起草单位：重庆燃气集团股份有限公司、昆仑能源有限公司、深圳市燃气集团股份有限公司、中国燃气控股有限公司、名气家（深圳）信息服务有限公司、唐山市天然气有限公司、重庆合众慧燃科技股份有限公司、北京中电华大电子设计有限责任公司、北京华虹集成电路设计有限责任公司、武汉大学、中国福州物联网开放实验室、北京智芯微电子科技有限公司、北京芯可鉴科技有限公司、北京握奇数据股份有限公司、上海飞奥燃气设备有限公司、金卡智能集团股份有限公司、杭州先锋电子技术股份有限公司、浙江威星智能仪表股份有限公司、浙江睿朗信息科技有限公司、新天科技股份有限公司、辽宁思凯科技股份有限公司、重庆市山城燃气设备有限公司、北京宏思电子技术有限责任公司、成都千嘉科技有限公司、成都秦川物联网科技股份有限公司、中国信息通信研究院-博鼎实华（北京）技术有限公司、东信和平科技股份有限公司、辽宁航宇星物联仪表科技有限公司、浙江苍南仪表集团股份有限公司、宁夏隆基宁光仪表股份有限公司、深圳友讯达科技股份有限公司、北京智慧云测设备技术有限公司

本标准主要起草人：……

本标准使用过程中如有建议或意见请联系中国城市燃气协会标准工作委员会秘书处或负责起草单位。负责起草单位：北京市燃气集团有限责任公司（地址：北京市西城区西直门南小街22号，邮政编码：100035，电子邮箱：jinjieyu@bjgas.com）

本标准由中国城市燃气协会制定，其版权为中国城市燃气协会所有。……

面向燃气物联网 NB-IoT 智能表的安全芯片检测技术规范

1. 范围

本文件规定了面向燃气物联网NB-IoT智能表的安全芯片（以下简称“安全芯片”）的检测内容、检测技术要求和检测方法。

本文件适用于城镇燃气行业NB-IoT智能表安全芯片的制造、检测、发行，及安全芯片嵌入式操作系统的研制、开发、集成和维护。

2. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2423.10 电工电子产品环境试验 第2部分:试验方法 试验Fc和导则:振动(正弦)

GB/T 2423.17 电工电子产品基本环境试验规程 第2部分:试验方法 试验Ka;盐雾试验方法

GB/T 2423.22 电工电子产品基本环境试验规程 试验N:温度变化试验方法

GB/T 4937.30 半导体器件 机械和气候试验方法 第30部分：非密封表面安装器件在可靠性试验前的预处理

GB/T 16649.3 识别卡集成电路 第3部分：带触点的卡 电气接口和传输协议

GB/T 17554.3 识别卡测试方法 第3部分：带触点的集成电路卡 及其相关接口设备

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 33133 信息安全技术 祖冲之序列密码算法

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 32918 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 38635 信息安全技术 SM9标识密码算法

GM/T 0008 安全芯片密码检测准则

3. 术语和定义、缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

安全芯片 Security chip

是一种支持 NB-IoT 燃气表安全应用的嵌入式集成电路。具有安全存储功能，安全通信功能，配合 COS 可以为上层应用提供基于密码技术的加解密、签名验签、摘要运算等密码运算功能，实现身份认证、通信加密、安全存储与安全访问的安全功能。

安全芯片包括独立式和嵌入式两类形态，其中独立式安全芯片提供安全应用和存储功能；嵌入式安全芯片代指高集成的多核协同芯片，其安全单元可与通信处理器、应用处理器、存储器等，通过系统级封装技术封装成一颗芯片。

注：本标准定义的安全芯片的通信接口仅适用于GB/T 16649 T=0通信协议标准。其他通信协议由应用方根据实际情况确定。

3.1.2

芯片 Chip

指安全芯片中用于完成数据处理和存储功能的集成电路器件。

3.1.3

集成电路（IC） integrated circuit(s) （IC）

用于执行处理或存储功能的电子器件。

3.1.4

字节 byte

由指明的 8 位数据 b1 到 b8 组成，从最高有效位（MSB，b8）到最低有效位（LSB，b1）。

3.1.5

报文 message

由智能燃气表发送给芯片（或反之）的一串字节，不包括传输控制字符。

3.1.6

报文认证码 message authentication code

对数据的一种对称加密变换，为保护数据发送方发出和接收方收到的数据不被第三方伪造。

3.1.7

公钥 public key

在一个实体使用的非对称密钥对中可以被公众使用的密钥。在数字签名方案中，公钥定义了验证函数。

3.1.8

加密 encipherment

基于某种加密算法对数据作可逆的变换从而生成密文的过程。

3.1.9

加密算法 cryptographic algorithm

隐藏或显现数据信息内容的变换算法。

3.1.10

解密 decipherment

对应加密过程的逆操作。

3.1.11

脚本 script

发行机构向安全芯片发送的命令或命令序列，目的是向安全芯片连续输入命令。

3.1.12

冷复位 cold reset

当接收到冷复位信号，安全芯片产生的复位。

3.1.13

密钥 key

加密转换中控制操作的一组符号。

3.1.14

密文 cryptogram

加密运算的结果。

3.1.15

密码 ciphertext

是一种用来混淆的技术，使用者用以将可识别的信息转变为无法识别的信息。

3.1.16

命令 command

终端向安全芯片发出的一条信息，该信息启动一个操作或请求一个应答。

3.1.17

热复位 warm reset

在已上电复位情况下，芯片因 reset 信号拉低后再拉高产生的复位。

3.1.18

签名 signature

对数据的一种非对称加密变换。该变换可以使数据接收方确认数据的来源和完整性，保护数据发送方发出和接收方收到的数据不被第三方篡改，也保护数据发送方发出的数据不被接收方篡改。

3.1.19

响应 response

安全芯片接收到命令报文经过处理后返回给智能燃气表的报文。

3.1.20

应用 application

安全芯片和智能燃气表之间的应用协议和相关的数据集。

3.1.21

关键指令 key commands

终端向安全芯片发出的一条或多条与燃气核心应用相关的重要信息，该信息启动一个或多个操作与请求应答。

例如：

报文认证命令；

读文件命令；

写文件命令；

加密命令；

解密命令；

扣款命令；

增款命令。

3.2 缩略语

以下缩略语和符号表示适用于本文件：

COS：芯片操作系统（Chip Operating System）

CLA：命令报文的类别字节（Class Byte of the Command Message）

CID：芯片唯一标识（Chip Unique Identification）

INS：命令报文的指令字节（Instruction Byte of Command Message）

I/O：输入/输出（Input/Output）

mA：毫安

MAC：报文认证码（Message Authentication Code）

RST：复位（Reset）

VCC：电源电压（Supply Voltage）

SM2：椭圆曲线公钥密码算法

SM3：杂凑密码算法

SM4：一种商用密码分组标准对称算法

SM9：一种标识密码算法

4. 对安全芯片的总体要求

4.1. 安全芯片的类型与架构

面向燃气物联网的NB-IoT智能表应支持独立式安全芯片或嵌入式安全芯片,要求分别如下。

a)独立式安全芯片应至少由安全模块、安全应用模块、存储模块、通信模块、电源模块、模拟模块、时钟模块、I/O模块等功能模块组成。独立式安全芯片的架构如图4.1所示。

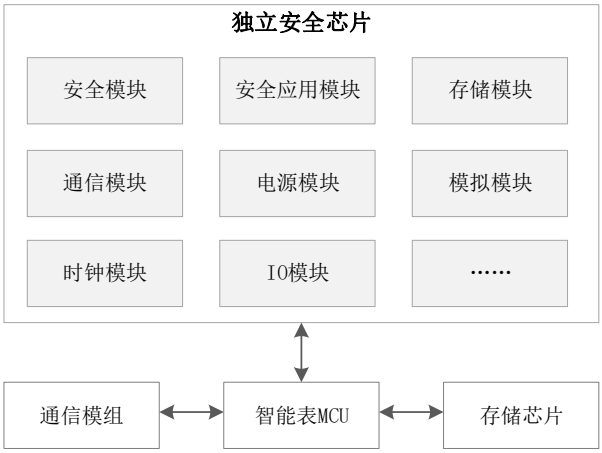

图4.1 独立式安全芯片架构

b)嵌入式安全芯片应至少由安全单元、通信处理器、应用处理器、电源管理单元、存储器、模拟电路模块等功能模块组成。其中，安全单元应至少包含安全模块、安全应用模块、存储模块、通信模块、传感模块。嵌入式安全芯片架构如图4.2所示。本规范对嵌入式安全芯片的要求主要针对安全单元。

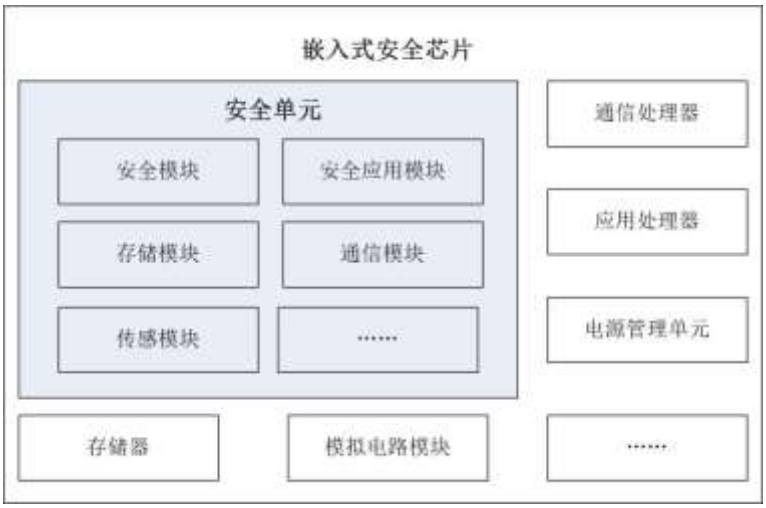

图 4.2 嵌入式安全芯片架构

c)对安全芯片检测条件与检测工具的要求参考本标准附录A；对安全芯片检测样本的要求参考本标准附录B。

4.2. 总体功能要求

a)应支持读取CID、更新密钥、交互报文、操作文件等基本指令，以实现安全应用和存储功能；

b)应能对接芯片发行系统，实现安全应用发行；

c)应支持NB-IoT智能表对指令处理逻辑和指令的输入参数进行检查,应能识别异常的处理逻辑和指令参数；

d)应支持透明二进制文件、记录文件等多种文件类型；

e)应支持多种安全访问方式和读写权限配置；

f)应支持安全数据传输，包括“密文+MAC”或“密文+签名”的传输方式；

g)应存储燃气智能终端身份认证流程及其算法体系相关的密钥等数据；

h)安全芯片通过其文件系统来支持数据的安全存储，可针对不同的存储数据，设置相应的安全策略，包括安全访问方式和读写权限配置、安全数据传输等。

4.3. 总体安全要求

a)独立式安全芯片应符合GM/T 0008二级及以上的要求；嵌入式安全芯片的安全等级宜符合GM/T 0008二级及以上的要求。

b)安全芯片的安全单元应符合GB/T 18336关于EAL4+认证的技术要求。

c)应支持国家商用密码管理规定要求的对称密码算法、杂凑算法、非对称密码算法。

d)应支持电压监测、温度监测等安全防护机制。

4.4. 总体性能要求

a)安全芯片非易失随机存储介质应能支持同一区域（物理页）连续执行至少5万次擦写操作；数据保存时间应大于10年，提供负载均衡策略，数据存储区擦写次数应大于50万次；

b)安全芯片基本指令应能稳定连续执行至少1万次；

c)国家商用密码算法相关功能应能稳定执行至少48小时；

d)各个阶段送检的样片应都能兼容各类主流机具，完成在各类主流机具上连续进行1万次关键指令和读写文件测试。

5. 安全芯片物理检测

5.1. 一般规定

安全芯片物理检测应从安全芯片外观、机械特征检测和电气特性等方面进行检测。

5.2. 外观检测

5.2.1. 检测内容

检测安全芯片的外观，判断其是否符合各项封装要求，主要包括封装体外观检测，管脚缺陷检测和关键尺寸检测等。

5.2.2. 检测方法

采用符合计量检测要求的数显卡尺、显微镜或其他标准封装量测工具对封装规格定义的芯片物理尺寸进行量测并记录。

5.2.3. 合格标准

封装体外观表面干净整洁、无划伤、缺角、丝印清晰；

管脚应排列整齐，无缺失、歪斜、长短不一致情况，表面应无可见氧化、变色、脏污；

关键尺寸检测符合封装规格要求定义范围。

5.3. 湿敏/回流焊检测

5.3.1. 检测内容

焊接热试验会使芯片中的潮气气压升高，从而导致塑封体破裂或电气性能失效。湿敏/回流焊检测通过模拟芯片在运输和存储环境中吸收的潮气，评价检测其耐焊接热性能。

5.3.2. 检测方法

芯片湿敏/回流焊检测方法遵循GB/T 4937.30标准。检测设备和材料应符合GB/T 4937.30中4.1至4.6规定。

按照如下流程对芯片进行检测，见GB/T 4937.30中5.5.2方法B：

a)初始功能和外观检测，见 GB/T 4937.30 中 5.2 初始测量；

b)125℃烘焙 24hr 去除封装内部水汽，见 GB/T 4937.30 中 5.4 干燥；

c)将干燥样品进行浸渍，见 GB/T 4937.30 中 5.5.2 表 2 里的干燥包装器件条件 B3 浸渍条件：30℃/60% RH，192hr；

d)回流焊 3 次循环，见 GB/T 4937.30 中 5.7 再流焊，其中回流焊过程的温度曲线设置需符合无铅装配回流标准曲线级别；

e)检测结束后功能和外观检测。

5.3.3. 合格标准

芯片通过湿敏/回流焊检测，检测结束后芯片功能达到规范要求，且没有外部裂纹。

5.4. 振动检测

5.4.1. 检测内容

模拟产品在运输、安装或使用环境下可能受到的各种振动环境影响，检测芯片是否能承受规定严酷等级的振动能力。

5.4.2. 检测方法

振动检测方法遵循GB/T 2423.10标准。

按照如下流程对芯片进行振动检测：

a)初始功能和外观检测；

b)将样品安装固定在振动台上，各项定义和试验要求见 GB/T 2423.10 中 3 和 4；

c)对样品实施扫频振动试验，见 GB/T 2423.10 中 8.3.1 和表 A.1，施加频率 f 为 5Hz~500Hz，X、Y、Z 三个轴方向各保持 25min 的正弦振动测试。

d)检测结束后功能和外观检测。

5.4.3. 合格标准

芯片通过频带范围内规定等级的振动检测，试验结束后芯片功能达到规范要求。

5.5. 高低温度变化检测

5.5.1. 检测内容

芯片产品在运输，储存以及使用过程中可能受到高低温度交替变化的温度应力，高低温度变化试验检测芯片产品耐受环境温度快速变化的能力。

5.5.2. 检测方法

芯片高低温度变化检测方法遵循GB/T 2423.22标准。试验箱及样品安装应符合GB/T 2423.22中8.2.1和8.2.2规定。

按照如下流程对芯片进行高低温度变化检测：

a)初始功能和外观检测；

b)将样品放入室温环境的试验箱；

c)高低温环境循环交替试验。见GB/T 2423.22试验Nb 8.2.3和8.2.5，低温环境为-25℃，高温环境为85℃，高温和低温环境下暴露持续时间分别为30min，高低温度间的转换时间小于1min，连续进行2个循环；

d)温度循环结束后待样品温度恢复。见GB/T 2423.22 中8.3；

e)检测结束后功能和外观检测。

5.5.3. 合格标准

芯片通过高低温热冲击检测，检测结束后芯片功能达到规范要求。

5.6. 盐雾试验检测

5.6.1. 检测内容

通过模拟盐雾环境条件，考核安全芯片抗盐雾腐蚀性能。

5.6.2. 检测方法

盐雾试验检测方法遵循GB/T 2423.17标准。检测设备和盐溶液应符合GB/T 2423.17中2和3的规定。

按照如下流程对芯片进行盐雾检测：

a)初始检测及清洁预处理。见 GB/T 2423.17 中 4 和 5 规定；

b)将样品放入盐雾试验箱进行试验。试验条件见 GB/T 2423.17 中 6 规定：采用温度为（35℃±2）℃，质量浓度为（5±1）%，PH 值在 6.5~7.2 之间（35℃±2℃）的氯化钠溶液，连续雾化试验 16hr；

c)将试验样品进行冲洗和干燥。见 GB/T 2423.17 中 7 规定；

d)试验结束后进行最终检测。

5.6.3. 合格标准

芯片通过盐雾试验检测，试验结束后芯片功能达到规范要求。

5.7. 芯片电气特性检测

5.7.1. 检测内容

检测安全芯片正常工作时VCC管脚、RST管脚、CLK管脚、IO管脚的输入电平电压、输入电流、信号上升沿上升时间、信号下降沿下降时间、管脚电容等电气特性的范围。

VCC 管脚：电源输入

RST 管脚：复位信号输入

CLK 管脚：时钟信号输入

GND 管脚：地（参考电压）

IO 管脚：串行数据的输入/输出

5.7.2. 检测方法

a）在检测设备上设置被测管脚的测试参数；

b）复位芯片；

c）运行一段测试程序，在通信过程中连续监测被测管脚的信号并记录电特性数据；

d）芯片下电；

e）对于芯片能支持的各档电压、各条件设置，重复步骤A）到D)。

关于VCC管脚的电气特性检测应遵循GB/T 17554.3中第6.1的规定。

关于IO管脚的电气特性检测应遵循GB/T 17554.3中第6.2的规定。

关于CLK管脚的电气特性检测应遵循GB/T 17554.3中第6.3的规定。

关于RST管脚的电气特性检测应遵循GB/T 17554.3中第6.4的规定。

5.7.3. 合格标准

1.正常操作条件下，VCC管脚的电气特性应符合表5-1的定义。

表 5-1 正常操作条件下 VCC 的电气特性

符号	条件	最小值	最大值	单位
U_{CC}	VCC=5V	4.5	5.5	V
	VCC=3V	2.7	3.3	
	VCC=1.8V	1.62	1.98	
I_{CC}	VCC=5V，在最大允许频率时		60	mA
	VCC=3V，在最大允许频率时		50	

	VCC=1.8V，在最大允许频率时		30	
电流值是 1ms 时间内的平均值。				

2. 正常操作条件下，RST管脚的电气特性应符合表5-3的定义。

表5-3 正常操作条件下RST的电气特性

符号	条件	最小值	最大值	单位
U_{IH}		$0.8U_{CC}$	U_{CC}	V
I_{IH}	U_{IH}	-20	+150	μA
U_{IL}		0	$0.12U_{CC}$	V
I_{IL}	U_{IL}	-200	+20	μA
t_R t_F	C_{IN}=30 pF		1	μs
注：RST 上的电压应保持在一 0.3V～U_{CC}+0.3V 之间。				

3. 正常操作条件下，CLK管脚的电气特性应符合表5-4的定义。

表 5-4 正常操作条件下 CLK 的电气特性

符号	条件	最小值	最大值	单位
U_{IH}		$0.7U_{CC}$	U_{CC}	V
I_{IH}	U_{IH}	-20	+100	μA
U_{IL}	VCC=5V 和 VCC=3V	0	0.5	V
I_{IL}	VCC=1.8V	0	$0.2U_{CC}$	V
	U_{IL}	-100	+20	μA
t_R t_F	C_{IN}=30 pF		时钟周期的 9%	μs
注：CLK 上的电压应保持在一 0.3V～U_{CC}+0.3V 之间。				

4. 正常操作条件下，IO管脚的电气特性应符合表5-5的定义。

表 5-5 正常操作条件下 I/O 的电气特性

符号	条件	最小值	最大值	单位
U_{IH}		$0.7U_{CC}$	U_{CC}	V
I_{IH}	U_{IH}	-300	+20	μA
U_{IL}		0	$0.15U_{CC}$	V
I_{IL}	U_{IL}	-1000	+20	μA
U_{OH}	外部上拉电阻：20 kΩ 到 U_{CC} 上	$0.7U_{CC}$	U_{CC}	V
I_{OH}	U_{HL} 和外部上拉电阻：20 kΩ 到 U_{CC} 上		+20	μA
U_{OL}	VCC=5V a 和 VCC=3V 类 a 时 IOL=1mA，VCC=1.8V 类 a 时 IOL=500μA	0	$0.15U_{CC}$	V
t_R t_F	C_{IN}=30pF；C_{OUT}=30pF		1	μs
注：I/O 上的电压应保持在一 0.3V～U_{CC}+0.3V 之间。				
a 接口设备的实现不应要求芯片吸入大于 500μA 的电流。				

注：详见GB/T16649.3 5.2对管脚电特性的规定。

6. 安全芯片通信协议检测

6.1. 一般规定

通信协议检测内容包括安全芯片字符帧编码检测、复位时序及逻辑检测、通信协议交互逻辑检测、通信速率检测等。应从底层硬件的角度检测安全芯片的通信协议，应保证安全芯片和终端的信息交换按照规范的要求可靠无误地进行。

6.2. 字符帧编码检测

6.2.1. 检测内容

检测安全芯片通信中字符帧编码、通信差错信号和字符重发的正确性。

6.2.2. 检测方法

a)将安全芯片与测试设备相连；

b)执行典型应用脚本与安全芯片进行通信；

c)使用测试工具测量通信过程中的字符帧收发情况并记录；

d)在典型应用脚本的典型位置构造字符帧接收差错信号，安全芯片应能够字符重发；

e)使用测试工具测量通信过程中的差错信号和字符重发情况并记录；

f)安全芯片下电。

6.2.3. 合格标准

安全芯片的数据字符帧编码应符合 GB/T16649.3 7.2 对字符帧编码的规定。

安全芯片对差错信号的处理和字符重发应符合 GB/T16649.3 7.3 对差错信号和字符重发的规定。

6.3. 复位时序及逻辑检测

6.3.1. 检测内容

检测安全芯片冷复位时序、热复位时序及复位应答的正确性。

6.3.2. 检测方法

a)将安全芯片与测试设备相连；

b)测试设备激活安全芯片；

c)使用测试工具连续监测冷复位期间VCC、RST、CLK、I/O信号的变化；

d)测试设备热复位安全芯片；

e)使用测试工具连续监测热复位期间VCC、RST、CLK、I/O信号的变化；

f)使用测试工具监测冷复位和热复位时安全芯片返回的复位应答的数据和时序；

g)安全芯片下电。

6.3.3. 合格标准

安全芯片的冷复位和热复位时序应符合 GB/T16649.3 6.2 对冷复位时序、热复位时序的规定。

安全芯片复位应答的字符和编码规则应符合 GB/T16649.3 8.1 对字符和编码的规定。

安全芯片复位应答 ATR 应符合 GB/T16649.3 8.2 对复位应答 ATR 的规定。

安全芯片复位应答的全局接口字节应符合 GB/T16649.3 8.3 对全局接口字节的规定。

6.4. 通信协议交互逻辑检测

6.4.1. 检测内容

检测安全芯片通信协议交互逻辑的正确性。

6.4.2. 检测方法

a)将安全芯片与测试设备相连；

b)执行脚本与安全芯片进行典型应用命令交互；

c)使用测试工具监测命令交互过程中的数据逻辑及时序；

d)安全芯片下电。

6.4.3. 合格标准

安全芯片通信协议交互的字符级应符合 GB/T16649.3 10.2 的规定。

安全芯片通信协议交互的命令结构和处理应符合 GB/T16649.3 10.3 的规定。

6.5. 通信速率检测

6.5.1. 检测内容

检测安全芯片通信速率的正确性。

6.5.2. 检测方法

a)将安全芯片与测试设备相连；

b)执行脚本与安全芯片进行速率协商；

c)使用测试工具监测速率协商的数据逻辑及时序；

d)执行脚本与安全芯片进行典型应用命令交互；

e)使用测试工具监测命令交互的速率；

f)安全芯片下电。

6.5.3. 合格标准

安全芯片的速率协商应符合 GB/T16649.3 中 9.2、9.3 的规定。

7. 安全芯片功能检测

7.1. 一般规定

应对安全芯片接收到的终端命令进行识别，校验每条命令的正确性，根据命令做出正确操作并给出相应响应。安全芯片在收到终端发来的不同命令时， 应识别当前命令属于安全芯片应用，交互流程应按照规范规定步骤进行，应校验每条命令的正确性，应根据命令做出正确操作并给出相应响应，遇到异常时应做出及时反馈。

应检测安全芯片燃气表安全应用功能的正确性，确保安全芯片的燃气表安全应用可以满足燃气业务应用需求。

7.2. 基本功能正确性检测

7.2.1. 检测内容

验证安全芯片燃气表安全应用基础功能的正确性。

7.2.2. 检测方法

对送检的安全芯片执行 CID 读取指令，安全芯片应返回芯片 CID，检测芯片 CID 长度、结构等符合燃气业务应用需求。

在满足相应权限及相应生命周期状态的条件下，对送检的安全芯片执行密钥更新指令，密钥应被更新成功，且使用新密钥执行相关指令操作应能成功，使用旧密钥执行相关指令操作应失败；对送检的安全芯片执行报文交互命令和文件操作命令，指令应被执行成功，且得到正确的响应和返回码。

7.2.3. 合格标准

CID 读取、密钥更新、报文交互命令和文件操作命令等基本指令功能符合燃气业务应用需求。

7.3. 文件系统检测

对安全芯片燃气表安全应用的文件系统进行检测，安全芯片应支持创建文件、读取文件、更新文件等文件系统操作指令。

7.3.1. 读取文件检测

7.3.1.1. 检测内容

验证存储在安全芯片燃气表安全应用文件系统内的数据应能被成功读取。

7.3.1.2. 检测方法

对送检的安全芯片执行读取文件指令，依次读取所有的文件内容，安全芯片应能够按照要求正确返回文件内容。

7.3.1.3. 合格标准

在满足相应权限及相应生命周期状态的条件下，安全芯片可以正确读取符合要求的文件内容。

7.3.2. 更新文件检测

7.3.2.1. 检测内容

验证存储在安全芯片燃气表安全应用文件系统中的文件内容应能被成功更新。

7.3.2.2. 检测方法

对送检的安全芯片执行更新文件指令，依次更新所有的文件内容，安全芯片应能够按照要求正确更新文件内容。

7.3.2.3. 合格标准

在满足相应权限及相应生命周期状态的条件下，安全芯片可以按要求正确更新文件内容。

7.4. 密码功能检测

7.4.1. 检测内容

应对安全芯片燃气表安全应用支持的密码功能进行检测。

7.4.2. 检测方法

a)对检测的安全芯片按照指定的对称密码算法工作模式对数据进行加解密，检测其运算结果正确性：

1)对给定的密钥和明文经指定的算法和工作模式加密，加密数据与给定密文完全相同；

2)对给定的密钥和密文经指定的算法和工作模式解密，解密数据和给定明文完全相同。

b)使用检测的安全芯片对消息进行杂凑运算，检测其运算结果正确性：

1)对给定消息调用杂凑算法计算杂凑值，计算结果和给定杂凑值完全相同；

2)对给定消息和参数调用杂凑算法计算杂凑值，计算结果和给定杂凑值完全相同。

c)对支持非对称密码算法的安全芯片进行数据进行签名/验签运算、加解密和密钥协商等运算，检测其运算结果正确性：

1)使用给定的密钥对待签名消息调用指定密码算法签名后，调用检测工具对该签名值进行验签运算，验签通过；

2)使用检测工具对给定的密钥和密码算法进行签名后，调用安全芯片对签名值进行验签，验签通过；

3)使用给定的密钥和明文调用指定密码算法加密后，调用检测工具对该加密结果进行解密，得到的结果与给定的明文完全相同；

4)使用给定的密钥和密文调用指定密码算法解密后，解密数据与给定明文完全相同；

5)使用给定的密钥和密钥协商参数，调用安全芯片密钥协商算法与检测工具进行密钥协商，协商结果正确。

7.4.3.合格标准

a)安全芯片燃气表安全应用支持至少一种对称密码算法，如分组密码算法、序列密码算法等。分组密码算法采用SM4算法时，其实现应符合GB/T 32907的要求；序列密码算法采用祖冲之算法时，其实现应符合GB/T 33133的要求；算法标识应符合GB/T 33560的要求。

b)安全芯片燃气表安全应用支持至少一种密码杂凑算法，宜支持带密钥的消息认证码HMAC生成。杂凑算法采用SM3算法时，其实现应符合GB/T 32905的要求；算法标识应符合GB/T 33560的要求。

c)安全芯片燃气表安全应用支持至少一种非对称密码算法，支持签名/验签运算、加解密、和密钥协商运算。非对称密码算法采用SM2算法时，其实现应符合GB/T 32918、GB/T 35275、GB/T 35276的要求；采用SM9算法时，其实现应符合GB/T 38635的要求；算法标识应符合GB/T 33560的要求。

7.5. 指令逻辑异常检测

7.5.1. 检测内容

验证安全芯片燃气表安全应用的指令异常处理逻辑应符合要求。

7.5.2.检测方法

对送检的安全芯片执行各类异常逻辑检测指令，检查安全芯片处理流程、边界检查、逻辑判断、返回的应答应符合要求。

7.5.3.合格标准

安全芯片燃气表安全应用指令具有异常处理逻辑，当安全芯片检测到各种异常情况时，需做出相应的处理及应答反馈。

7.5.3.1.密钥更新

在满足相应权限及相应生命周期状态的条件下，应符合以下标准:

a)密钥更新指令未进行完整性校验时，密钥更新指令执行失败，新密钥不可使用，旧密

钥可正常使用。

b)密钥更新指令完整性校验错误时，密钥更新指令执行失败，新密钥不可使用，旧密钥可正常使用。

c)密钥更新指令中密钥类型错误时，密钥更新指令执行失败，新密钥不可使用，旧密钥可正常使用。

d)密钥更新指令中密钥长度错误时，密钥更新指令执行失败，新密钥不可使用，旧密钥可正常使用。

e)密钥更新指令中密钥索引错误时，密钥更新指令执行失败，新密钥不可使用，旧密钥可正常使用。

7.5.3.2. 更新文件

a)对于有权限限制的文件，未通过相应密钥认证获取到更新文件权限，更新文件不成功且返回异常应答反馈。

b)对于不可更新的文件，执行更新文件指令不成功且返回异常应答反馈。

c)当文件类型不存在时，执行更新文件指令不成功且返回异常应答反馈。

d)当文件类型不匹配时，执行更新文件指令不成功且返回异常应答反馈。

e)当文件属性要求签名更新文件时：

1)若未进行签名，执行更新文件指令不成功且返回异常应答反馈。

2)若签名错误的情况下，执行更新文件指令不成功且返回异常应答反馈。

f)当文件属性要求更新文件带完整性校验时：

1)若未进行完整性校验，执行更新文件指令不成功且返回异常应答反馈。

2)若完整性校验错误，执行更新文件指令不成功且返回异常应答反馈。

7.5.3.3. 读取文件

a)对于有权限限制的文件，未通过相应密钥认证获取到读文件权限，则读取文件不成功且返回异常应答反馈。

b)对于不可读的文件，执行读文件指令不成功且返回异常应答反馈。

c)当文件类型不存在时，执行读文件指令不成功且返回异常应答反馈。

d)当文件不存在时，执行读文件指令不成功且返回异常应答反馈。

e)当文件属性要求签名读文件时，若未进行签名，执行读文件指令不成功且返回异常应答反馈。

f)当文件属性要求签名读文件时，若签名错误的情况下，执行读文件指令不成功且返回

异常应答反馈。

g)当文件属性要求更新文件带完整性校验时，若未进行完整性校验，执行读文件指令不成功且返回异常应答反馈。

h)当文件属性要求更新文件带完整性校验时，若完整性校验错误，执行读文件指令不成功且返回异常应答反馈。

7.5.3.4. 密码功能

a)当密钥错误的情况下，执行密码功能相关指令不成功且返回异常应答反馈。

b)当密钥不存在的情况下，执行密码功能相关指令不成功且返回异常应答反馈。

c)要求完整性校验的指令，在未进行完整性校验码的情况下，执行密码功能相关指令不成功且返回异常应答反馈。

d)要求完整性校验的指令，在完整性校验错误的情况下，执行密码功能相关指令不成功且返回异常应答反馈。

e)要求签名的指令，在签名不存在的情况下，执行密码功能相关指令不成功且返回异常应答反馈。

f)要求签名的指令，在签名错误的情况下，执行密码功能相关指令不成功且返回异常应答反馈。

7.6. 指令参数检查

7.6.1. 检测内容

验证安全芯片燃气表安全应用的指令参数应符合要求。

7.6.2. 检测方法

根据每一个参数除正常值以外的其他值分别组成参数检查指令，逐一对送检的安全芯片执行该指令，安全芯片不应执行正常逻辑处理，且应返回异常应答反馈。

7.6.3. 合格标准

安全芯片燃气表安全应用指令具有参数检查功能，即当安全芯片检测接收到的指令参数不符合要求时应做出相应的处理及应答反馈。

7.7. 生命周期检测

7.7.1. 检测内容

验证安全芯片燃气表安全应用生命周期管理功能的正确性。

7.7.2. 检测方法

对送检的安全芯片执行生命周期状态切换指令，生命周期状态应能按顺序切换成功，

且在所属生命周期内安全芯片的功能应正确。

检测安全芯片生命周期状态切换到应用态时，生命周期状态应不可回退。

7.7.3. 合格标准

安全芯片具备生命周期管理及生命周期状态切换功能，安全芯片各生命周期状态功能应正常、安全性应符合要求。

7.8. 原子性检测

7.8.1. 检测内容

验证安全芯片在执行命令过程中断电的情况下，安全芯片非易失性存储器内数据不会发生错误。

7.8.2. 检测方法

对送检的安全芯片执行更新文件、密钥更新等命令，在命令执行过程中断电，检查被写文件数据内容，数据内容应与待写入数据或原数据完全一致。

7.8.3. 合格标准

安全芯片具备断电保护功能，保证断电执行过程中的数据的一致性。

7.9. 应用功能稳定性检测

应对安全芯片燃气表安全应用的功能稳定性进行检测，检测项应包含基础功能稳定性检测、文件读写稳定性检测、密码功能稳定性检测三个子项。

7.9.1. 基础功能稳定性检测

7.9.1.1. 检测内容

验证安全芯片燃气表安全应用基础功能的稳定性。

7.9.1.2. 检测方法

对送检的安全芯片重复执行燃气表安全应用基础功能指令，重复执行 1 万次，每次操作都应成功被执行，且执行结果正确。

7.9.1.3. 合格标准

安全芯片内的燃气表安全应用基础功能运行稳定。

7.9.2. 文件读写稳定性检测

7.9.2.1. 检测内容

验证安全芯片燃气表安全应用文件读写功能的稳定性。

7.9.2.2. 检测方法

对送检的安全芯片重复执行燃气表安全应用文件读写指令，重复执行 1 万次，每次操

作都应成功被执行，且执行结果正确。

7.9.2.3. 合格标准

安全芯片内的燃气表安全应用文件读写功能运行稳定。

7.9.3. 密码功能稳定性检测

7.9.3.1. 检测内容

验证安全芯片燃气表安全应用密码功能的稳定性。

7.9.3.2. 检测方法

对送检的安全芯片重复执行燃气表安全应用密码功能指令，持续执行 48 小时，每次操作都应成功被执行，且执行结果正确。

7.9.3.3. 合格标准

安全芯片内的燃气表安全应用密码功能运行稳定。

7.10. 发行功能检测

7.10.1. 检测内容

验证已完成个性化发行的安全芯片燃气表安全应用功能的正确性。

7.10.2. 检测方法

检测人员应使用发行工具发行安全芯片并进行检测。

发行成功后，须确认成功发行的安全芯片的文件结构建立正确，密钥写入正确，权限使能正确。

a) 判断存储数据的正确性，发行工具写入的个性化数据全部读出并进行对比，读出的数据应与写入的数据一致。

b) 要求必须权限验证通过才能读取的文件内容，未通过验证，读取文件应失败。

c) 要求必须权限验证通过才能读取的文件内容，验证成功，读取文件应成功。

d) 要求必须权限验证通过才能更新的文件内容，未通过验证，更新文件应失败，应读出原始数据内容。

e) 要求必须权限验证通过才能更新的文件内容，验证成功，更新文件应成功，应读出更新后的数据内容。

f) 要求带签名更新的文件内容，没有签名进行写操作，更新文件应失败，应读出原始数据内容。

g) 要求带签名更新的文件内容， 签名错误，更新文件应失败，应读出原始数据内容。

h) 要求带签名更新的文件内容， 签名正确，更新文件应成功，应读出更新后的数据

内容。

i) 对安全芯片的所有指令进行功能正确性检测，应执行成功。

7.10.3. 合格标准

已完成个性化发行的安全芯片文件结构、个性化数据、燃气表安全应用功能正常。

8. 安全芯片性能检测

8.1. 一般规定

应通过专用设备对安全芯片进行关键指令性能检测、疲劳性检测等。

8.2. 关键指令性能检测

8.2.1. 检测内容

验证安全芯片燃气表安全应用的关键指令的性能指标。

8.2.2. 检测方法

使用性能检测工具，根据关键指令性能指标公式计算关键指令成功执行的处理时间。宜重复 100 轮以上计算其平均时间。

8.2.3. 合格标准

安全芯片燃气表安全应用的关键指令性能指标满足要求。关键指令性能指标计算公式为：关键指令成功执行的处理时间=指令执行总时间-通信时间。

8.3. 密码算法性能检测

8.3.1. 检测内容

验证安全芯片燃气表安全应用提供的密码功能的性能，安全芯片燃气表安全应用的算法性能检测应包括以下几个方面：对称算法的加解密性能、杂凑算法运算性能，宜包括非对称算法的加解密性能、非对称算法签名及验签性能。

8.3.2. 检测方法

a)对称算法加解密性能：将一个字节长度为 L 的数据报文，发送给安全芯片进行加/解密操作，重复操作 100 轮执行成功，统计其完成时间。根据对称算法加解密指标公式计算其性能；

b)非对称算法加解密性能：将一个字节长度为 L 的数据报文，发送给安全芯片进行加密/解密操作，重复操作 100 轮执行成功，统计其完成时间。根据非对称算法加解密指标公式计算其性能；

c)非对称算法签名及验签性能：将一个字节长度为 L 的数据报文，发送给安全芯片进行签名操作，重复操作 100 轮执行成功，统计其完成时间，根据非对称算法签名及验签性能指标公式计算其签名性能。将签名后的数据报文，发送给安全芯片进行验签操作，重复操 100 轮执行成功，统计其完成时间，根据非对称算法签名及验签性能指标公式计算其验签性能；

d)杂凑算法运算性能：将一个字节长度为 L 的数据报文，发送给安全芯片进行摘要运算，重复操作 100 轮执行成功，统计其完成时间。根据杂凑算法运算性能指标公式计算其性

能。

8.3.3. 合格标准

限定 L 为安全芯片燃气表安全应用单包数据报文可发送的最大长度。

a)对称算法加解密性能计算标准：将一个字节长度 L 的数据报文，发送给安全芯片进行加/解密操作，重复操作 N 次执行成功，测试其完成时间 T 秒。需根据燃气安全应用所支持的对称算法工作模式的性能。性能指标计算公式为：S=8LN/（1024×1024T）；单位为 Mbps；

b)非对称算法加密/解密性能计算标准：将一个字节长度 L 的数据报文，发送给安全芯片进行加密/解密操作，重复操作 N 次执行成功，测试其完成时间 T 秒。性能指标计算公式为：S=8LN/（1024T）；单位为 Kbps；

c)非对称算法签名/验签性能计算标准：将一个字节长度 L 的数据报文，发送给安全芯片进行签名/验证操作，重复操作 N 次执行成功，测试其完成时间 T 秒。性能指标计算公式为：S=N/T；单位为（次/秒）；

d)杂凑算法运算性能计算标准：将一个字节长度 L 的数据报文，发送给安全芯片进行摘要运算，重复操作 N 次执行成功，测试其完成时间 T 秒。性能指标计算公式为：S=8LN/（1024×1024T）；单位为 Mbps。

8.4. 疲劳性检测

应对安全芯片的非易失随机存储介质的抗疲劳能力进行检测。

8.4.1. 检测内容

验证安全芯片非易失随机存储介质的抗疲劳能力。

安全芯片采用页模式管理的存储介质时，验证介质支撑跨页读写功能以及擦写寿命。

8.4.2. 检测方法

对安全芯片非易失随机存储介质的同一区域连续执行 5 万次读写操作，写操作每次都能成功被执行，且每次读出来的数据都正确无误。

若存储介质采用页式存储管理，则根据其页大小，建立文件跨页测试，对同一区域连续执行 5 万次写操作，写操作每次都能成功被执行，且每次读出来的数据都正确无误。

8.4.3. 合格标准

对安全芯片连续进行高强度操作，安全芯片功能不会发生紊乱。

若采用页模式管理的存储介质，支持跨页读写功能，擦写寿命满足 5 万次。

支持负载均衡策略，数据存储区擦写寿命大于 50 万次；

对安全芯片数据存储区连续 50 万次读写操作，写操作每次都能成功被执行，且每次读

出来的数据都正确无误。

9. 安全芯片安全性检测

9.1. 一般规定

安全芯片安全性检测的总体要求，应包括发行功能检测、敏感信息存储安全检测、密码运算安全性检测、逻辑异常攻击检测、后门命令检测、安全审计检测、芯片 ID 唯一性检测、随机数随机性检测和重放攻击检测等。

9.2. 发行功能检测

9.2.1. 检测内容

发行功能应检测文件的结构、大小、类型，读写权限，芯片的存储空间、指令集指令功能、生命周期及密钥发行的正确性、完整性。

9.2.2. 检测方法

a) 安全芯片的预发行，应检测文件系统的文件结构、文件类型和文件大小符合相应的规范，能够为数据的写入提供应有的存储空间和预发行权限；

b) 安全芯片的密钥发行，应该确保在安全可控的环境下进行，安全芯片需要满足相应的密钥发行权限，才可以进行密钥发行；

c) 应逐条检测送检单位提供的安全芯片初始化指令集，检测指令功能与 COS 说明文档描述一致；

d) 检测评估对象应有一定的生命周期维护功能，当生命周期切到用户模式的时候，确保生命周期的切换生效；

e) 完成预发行后的安全芯片，确保密钥发行的完整性、正确性，初始化数据的完整性、正确性，与期望的初始化信息一致；

9.2.3. 合格标准

安全芯片发行应确保安全可控的进行密钥发行和数据写入，生命周期的管理应符合相应的业务安全规范，保证发行的安全芯片不会泄漏敏感信息。

9.3. 敏感信息存储安全

9.3.1. 检测内容

敏感信息检测内容应包括密钥、安全状态、生命周期、燃气表配置参数。

9.3.2. 检测方法

a) 应审查、确认安全信息的内容。敏感信息的写入和维护应满足生命周期的状态约束；

b) 若密钥是通过密钥文件存储在非易失存储介质中，密钥文件应不可读出；

c) 安全芯片应用状态下如有写权限要求的文件，必须在特定权限下才能写入。

9.3.3. 合格标准

安全芯片对密钥、安全状态、生命周期、燃气表配置参数等敏感信息应该采用安全的方式存储与管理，具有安全保护机制，不可泄露。在非安全可控的条件下不可修改或者读写敏感信息、导出非对称公钥相关信息，禁止导出上下行密钥。

9.4. 密码运算安全性检测

9.4.1. 检测内容

密码运算安全性检测应对涉及密码运算可能导致旁路攻击漏洞的对称算法、非对称算法进行检测。

9.4.2. 检测方法

检测一：对称算法

a) 对样片进行波形采集，采集的波形应包括对称算法整体运算部分。

d) 应对采集的波形进行分析，与厂家提供的材料中描述的防护方案进行比较，确认厂家提交的安全芯片和材料是真实可信的。

e) 应大量采集芯片运算对称算法的波形，对其进行攻击，形成内部记录文档。

f) 应大量采集芯片在对称密钥导入过程中的波形，对其进行模板分析攻击，形成内部记录文档。

检测二：非对称算法

a) 对样片进行波形采集，采集的波形应包括非对称算法整体运算部分。

b) 应对采集的波形进行分析，与厂家提供材料中描述的防护方案进行比较，确认厂家提交的安全芯片和材料是真实可信的。

c) 应根据采集的波形，针对非对称的点乘部分进行攻击，形成内部记录文档。

d) 应根据采集的波形，针对非对称的私钥运算部分进行攻击，形成内部记录文档。

9.4.3. 合格标准

密码算法的运算过程可防旁路攻击，满足安全芯片的安全保护措施。嵌入式安全芯片应至少符合 GM/T 0008 二级要求。独立式安全芯片应至少符合 GM/T 0008 二级要求。

9.5. 逻辑异常攻击检测

9.5.1. 检测内容

逻辑异常攻击检测应检测安全芯片在接收到一定规模的非预期输入后是否会泄露敏感信息。

9.5.2. 检测方法

应审查安全芯片的命令指令集，输入非预期命令序列以外的随机指令，安全芯片不应泄露敏感信息。

9.5.3. 合格标准

安全芯片的功能不应受逻辑异常的影响，包括但不限于：非预期命令序列，未知命令，错误参数或数据等等可能会导致安全芯片功能紊乱或输出敏感信息的逻辑异常。

9.6. 后门命令检测

9.6.1. 检测内容

后门命令检测应检测安全芯片是否存在未公开的后门命令。

9.6.2. 检测方法

安全芯片应用状态下应对 CLA（00-FF），INS（00-FF）进行扫描，对安全芯片的指令集中没有声明的指令应返回‘6D00’或‘6E00’。

9.6.3. 合格标准

安全芯片中不应该存在未公开的命令，导致安全芯片敏感信息的泄露。评估对象的设计和执行应保证发行的芯片不会导致安全芯片敏感信息的泄露。

9.7. 安全审计检测

9.7.1. 检测内容

安全审计检测应检测安全芯片是否具备记录指令执行及结果的能力。

9.7.2. 检测方法

对审计对象，执行测试指令，查看安全芯片中是否有相应的执行结果信息。

9.7.3. 合格标准

安全芯片应提供安全审计功能，来记录安全相关的事件，以便帮助管理者发现潜在的攻击和由于评估对象的安全特性的错误配置使之陷入易被攻击的状态。

审计功能应给安全芯片管理者提供机会，回顾之前的操作信息，以确定评估对象是否受到过攻击；记录数据应包括芯片执行的指令和执行结果。

9.8. CID 唯一性检测

9.8.1. 检测内容

CID唯一性检测应检测安全芯片标识是否唯一。

9.8.2. 检测方法

在芯片的发行阶段，通过发行系统确认 CID 的唯一性。

9.8.3. 合格标准

安全芯片标识 CID 应唯一。

9.9. 随机数随机性检测

9.9.1. 检测内容

随机数随机性检测应检测随机数的随机性是否能通过 GM/T 0008 的检测标准。

9.9.2. 检测方法

安全芯片应连续执行随机数生成指令，生成 128M 随机数文件。

9.9.3. 合格标准

随机数发生器应具有足够的随机性，其随机性指标应通过 GM/T 0008 检测标准的检测。

9.10. 重放攻击检测

9.10.1. 检测内容

重放攻击检测应检测安全芯片是否能防止历史命令的重放执行。

9.10.2. 检测方法

安全芯片应满足相关技术安全规范的要求，可以有效防范报文的重放攻击，计数器、时间戳、随机数等设计应满足防重放攻击要求，随机数应确保采用真随机，如有条件随机数应该由硬件设备或者芯片产生，交互流程中确保随机数的新鲜性，重复执行的重放攻击指令，应失败。

9.10.3. 合格标准

安全相关的关键处理流程，应可防止重放攻击，满足相应的安全芯片技术规范要求。

10. 安全芯片可靠性检测

10.1. 高温工作寿命试验（HTOL）

10.1.1. 检测内容

进行高温工作寿命试验，考核产品在规定条件下全寿命工作时间内的可靠性，发现温度/电压加速失效机理，并预估长期的失效率。

10.1.2. 检测方法

a)检测前确认样品功能正常；

b)样品放入高温烘箱，在高温运行过程中，需运行合适的功能测试程序或测试向量，以保证尽可能多的晶体管处于翻转状态。根据检测等级选取以下其中一个条件进行测试，条件1：环境温度85℃，电源电压为Vccmax，检测时间1000h；条件2：环境温度105℃，电源电压为Vccmax，检测时间1000h；条件3：环境温度125℃，电源电压为Vccmax，检测时间1000h；条件4：环境温度150℃，电源电压为Vccmax，检测时间1000h；

c)常温冷却2小时后，168小时内检测样品功能是否正常。

10.1.3. 合格标准

在检测后进行功能及性能测试,所有被测样品功能及电特性指标符合规格要求视为通过。

10.2. 低温工作寿命试验（LTOL）

10.2.1. 检测内容

进行低温工作寿命试验，考核产品在规定条件下全寿命工作时间内的可靠性，发现热/电压加速失效机理，预估长期的失效率。

10.2.2. 检测方法

a)检测前确认样品功能正常；

b)样品放入低温箱，在低温运行过程中，需运行合适的功能测试程序或测试向量，以保证尽可能多的晶体管处于翻转状态。根据检测等级设定环境温度为-25℃，电源电压为Vccmax，检测时间1000h；

c)恢复常温2小时后，168小时内检测样品功能是否正常。

10.2.3. 合格标准

在检测后进行功能及性能测试，所有被测样品功能及电特性指标符合规格要求视为通过。

10.3. 高温读写＋保存数据退化检测（High Temp NVCE + PCHTDR）

10.3.1. 检测内容

进行高温下的读写操作和数据保存退化测试，本检测主要考核存储器单元在高温环境下的长期读写擦除及数据保存能力。

10.3.2. 检测方法

a)检测前确认样品功能正常；

b)样品处于写－读－擦除模式下循环检测，根据检测等级设定结温 Tj1=85℃，擦写次数参考 8.4.2 要求（必须在 500 小时内完成）；

c)样品写入校验数据，检验数据可以写全 0、全 1、棋盘格、反棋盘格等类型数据；

d)样品在数据擦写完成后，根据检测等级设定结温 Tj2=125℃，进行保存数据退化检测。对于进行了 100%最大擦写次数的存储单元，保存 10 小时，对于进行了≤10%最大擦写次数的存储单元，保存 100 小时；

e)读取样品数据，并与校验数据对比；

f)检测样品功能是否正常。

10.3.3. 合格标准

在检测后进行功能及性能测试，校验数据需保持一致，所有被测样品功能及电特性指标符合规格要求视为通过。

10.4. 常温读写＋保存数据退化检测（Room Temp NVCE + LTDDR）

10.4.1. 检测内容

进行常温下的读写和数据只读测试，本检测主要考核存储器单元在常温环境下的长期读写擦除及数据保存能力。

10.4.2. 检测方法

a)检测前确认样品功能正常；

b)样品处于写－读－擦除模式下循环检测，结温在 25 度，循环 5 万次（必须在 500 小时内完成）；

c)样品写入校验数据，检验数据可以写全 0、全 1、棋盘格、反棋盘格等类型数据；

d)样品在结温在 25 度，只读取数据，进行 500 小时；

e)读取样品数据，并与校验数据对比；

f)检测样品功能是否正常。

10.4.3. 合格标准

在检测后进行功能及性能测试，校验数据需保持一致，所有被测样品功能及电特性指标

符合规格要求视为通过。

10.5. 预处理试验（PC）

10.5.1. 检测内容

预先模拟芯片从出厂运输条件下的温湿度存储环境到单板 SMT 生产加工等场景下封装的可靠性。

10.5.2. 检测方法

a)检测前确认样品功能正常；

b)样品放入高温烘箱，检测条件：125℃，24 小时；

c)样品放入温湿度箱，检测条件：30 ℃ / 60% RH，192 小时

d)样品进行回流焊，回流焊条件：无铅焊接曲线，260 ℃，3 次；

e)检测样品功能是否正常。

10.5.3. 合格标准

在检测后进行功能及性能测试，所有被测样品功能及电特性指标符合规格要求视为通过。

10.6. 高加速温湿度寿命检测（uHAST）

10.6.1. 检测内容

在高温高湿高压条件下检验塑封封装产品抗水汽侵入并腐蚀的能力，评估芯片在施加高温、高湿、高气压条件下的封装对湿气的抵抗能力。这些组合应力会在化学反应失效机理下加速封装材料的失效过程。

10.6.2. 检测方法

a)检测前确认样品功能正常；

b)进行预处理试验（PC）；

c)预处理试验完成后检测样品功能是否正常；

d)检测条件 130℃、85%RH、VP = 230kPa、96h；

e)检测样品功能是否正常。

10.6.3. 合格标准

在检测后进行功能及性能测试，所有被测样品功能及电特性指标符合规格要求视为通过。

10.7. 静电防护-人体模型试验（ESD-HBM）

10.7.1. 检测内容

模拟人体放电的电流波形，按规定的组合及顺序对器件各引出端放电，检验产品承受静电放电的能力。

10.7.2. 检测方法

a)检测前确认样品功能正常；

b)根据样品标称值进行检测，测试电压等级≥±2000V。

c)检测完成后检测样品功能是否正常。

10.7.3. 合格标准

在检测后进行功能及性能测试，所有被测样品功能及电特性指标符合规格要求视为通过。

10.8. 静电防护-器件充电模型试验（ESD-CDM）

10.8.1. 检测内容

模拟器件积累静电荷后被金属工具接触产生的放电电流波形，按规定的组合及顺序对器件各引出端放电，检验产品承受静电放电的能力。

10.8.2. 检测方法

a)检测前确认样品功能正常；

b)根据样品标称值进行检测，测试电压等级≥±500V。

c)检测完成后检测样品功能是否正常。

10.8.3. 合格标准

在检测后进行功能及性能测试，所有被测样品功能及电特性指标符合规格要求视为通过。

10.9. 闩锁试验（Latch-up）

10.9.1. 检测内容

检测芯片各个管脚不发生闩锁的阈值电压和电流，检验芯片的抗闩锁设计能力。

10.9.2. 检测方法

a)检测前确认样品功能正常；

b)常温下，对于电压管脚，进行 1.5*Vcc Max 或 MSV 检测；

c)常温下，对于 IO 管脚，进行±100mA 的电流检测；

10.9.3. 合格标准

a)试验过程中不发生闩锁效应；

b)在检测后进行功能及性能测试，所有被测样品功能及电特性指标符合规格要求视为通过。

11. 安全芯片兼容性和一致性检测

11.1. 物理稳定性和物理兼容性检测

11.1.1. 检测内容

安全芯片应能够在发行机具和业内各种主流机具上稳定工作。

11.1.2. 检测方法

安全芯片在发行机具和业内各种主流机具上分别进行 1 万次关键指令和读写文件测试，检测每条指令都应执行成功。

11.1.3. 合格标准

安全芯片在发行机具和业内至少 2 种主流机具上可稳定工作，且具有良好的兼容性。

11.2. 上线发行检测

11.2.1. 检测内容

使用发行系统对安全芯片下载应用并进行个性化，检测安全芯片的功能。

11.2.2. 检测方法

a)存储数据正确性检测：发行系统写入的个性化数据全部读出进行对比；

b)文件检测：选择安全芯片所有的文件，并对文件进行正确安全权限的操作，检测所有文件的读写权限、文件属性是否正确；

c)密钥正确性检测：对安全芯片进行密码运算，结果应正确；

d)应用功能检测：通过发行系统发行的安全芯片，应用功能应与通过检测环境发行的安全芯片各类指标和功能一致。

11.2.3. 合格标准

与发行系统对接稳定，通过发行系统发行出的安全芯片与通过检测环境发行的安全芯片各类指标和功能一致。

11.3. 一致性检测

11.3.1. 检测内容

不同阶段送检的安全芯片应保持一致，应保持安全芯片的基本功能、主要参数等因素与送检厂家备案的功能相同，且与送检厂家备案的芯片型号和 COS 相关证书的信息一致。

11.3.2. 检测方法

a)基本功能检测：对送检安全芯片进行基本功能正确性检测；

b)时序一致性检测：要求各批次送检安全芯片与送检备案时提交的芯片时序保持一致，

包括复位时序，关键指令时序；

c)功耗一致性检测：采集关键指令的波形留存，对比波形确定安全芯片一致性；

d)芯片物理特性一致性：检测各批次送检安全芯片物理特性是否符合一致性检测要求，要求与备案时提交的参数保持一致；

e)芯片应用功能一致性检测：检测安全芯片应用功能是否符合一致性检测要求，要求正式发行前送检的安全芯片与备案时出具的检测报告结果保持一致。

11.3.3. 合格标准

对样品安全芯片进行一致性检测，确保各阶段送检的安全芯片与备案时声明的各项信息一致，以及发行前送检的安全芯片与最终出具的检测报告的安全芯片保持一致。

附录 A 安全芯片检测条件与检测工具要求

A.1 检测条件

默认环境条件（温度，湿度等）是指常温 20±3℃，湿度 20%-80%之间。如无特殊说明，默认检测均采用此环境条件。

A.2 检测工具

A.2.1 安全芯片物理检测与通信协议检测工具

- 光学显微镜：用于外观检测、湿敏/回流焊检测
- 数显卡尺等标准封装量测工具：用于外观检测
- 潮湿箱：用于湿敏/回流焊检测
- 焊接设备：用于湿敏/回流焊检测
- 干燥箱：用于湿敏/回流焊检测
- 温度循环箱：用于高低温热冲击检测、湿敏/回流焊检测
- 振动试验台：用于振动检测
- 盐雾箱：用于盐雾试验检测
- 电学测试设备（如压力表、电流表等）：用于电特性测试
- 接触协议测试仪：用于通信协议测试

A.2.2 安全芯片功能检测、性能检测工具

- 标准 PCSC 读卡器：用于通过 ISO 7816 协议对安全芯片进行读写操作
- 性能检测仪：用于对安全芯片进行性能检测
- 面向燃气物联网 NB-IoT 智能表的安全芯片应用检测系统：用于对安全芯片进行功能检测、性能检测检测

A.2.3 安全芯片安全性检测工具

- 安全芯片读写设备及软件（接口板卡及逻辑协议分析套件）：用于常规读写逻辑正确性与安全性检测。
- 安全攻击分析设备及软件（芯片功耗采集设备、电磁探头、电流探头、光攻击等错误注入设备，示波器、前置放大器、移动台、SCA 分析软件等）：用于 SCA 与注错攻击测试。
- 能够支持国密二级的类似 NIST 检测工具：用于检测随机数。

A.2.4 安全芯片可靠性检测工具

- 高低温试验箱：用于高温工作寿命试验、低温工作寿命试验、高温读写＋保存数据退化检测、常温读写＋保存数据退化检测
- 直流稳压电源：用于预处理试验
- 高低温交变湿热试验箱：用于预处理试验
- 回流焊设备：用于预处理试验
- 高加速压力偏压系统：用于高加速温湿度寿命检测
- 静电栓锁试验仪：用于静电防护-人体模型试验、闩锁试验
- 充放电测试仪：用于静电防护-器件充电模型试验

A.2.5 安全芯片兼容性和一致性检测工具

- 标准 PCSC 读卡器：用于通过 ISO 7816 协议对安全芯片进行读写操作
- 接触式读卡器模拟器：用于监测和芯片之间的 ISO 7816 协议数据并解析
- 面向燃气物联网 NB-IoT 智能表的安全芯片应用检测系统：用于对安全芯片进行兼容性和功能一致性检测
- 时序测试软件：用于对安全芯片的时序一致性进行检测

附录 B 安全芯片检测样本要求

检测项目	样本要求	
	Class A	Class B
高温工作寿命试验（HTOL）	1个批次，77颗	3个批次，每个批次77颗
低温工作寿命试验（LTOL）	1个批次，32颗	3个批次，每个批次32颗
高温读写＋保存数据退化检测（High Temp NVCE + PCHTDR）	1个批次，39颗	3个批次，每个批次39颗
常温读写＋保存数据退化检测（Room Temp NVCE + LTDDR）	1个批次，38颗	3个批次，每个批次38颗

预处理试验（PC）	1个批次，25颗	3个批次，每个批次25颗
高加速温湿度寿命检测（uHAST）	1个批次，25颗	3个批次，每个批次25颗
静电防护-人体模型试验（ESD-HBM）(1)	3颗	6颗
静电防护-器件充电模型试验（ESD-CDM）(2)	3颗	6颗
闩锁试验（Latch-up）(3)	3颗	6颗
一致性测试	3颗	
注（1）：参考IEC 60749-26标准； 注（2）：参考IEC 60749-28标准； 注（3）：参考IEC 60749-29标准。		