ICS
CCS

团　　体　　标　　准

T/CAAMTB xx－20xx

汽车控制芯片功能安全 ASIL 等级技术要求及评估方法

Technical requirements and evaluation methods for ASIL level of functional safety of automotive control chips

20xx-xx-xx 发布　　20xx-xx-xx 实施

中国汽车工业协会 发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由中国汽车工业协会标准法规工作委员会汽车芯片专业委员会提出。

本文件由中国汽车工业协会归口。

本文件起草单位：

本文件主要起草人：

汽车控制芯片功能安全ASIL等级技术要求及评估方法

1 范围

本文件规定了针对不同控制芯片功能安全ASIL等级的技术要求及评估方法。

本文件适用于汽车控制芯片功能安全的设计和评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 34590（所有部分） 道路车辆 功能安全

3 术语和定义

GB/T 34590.1—2022界定的以及下列术语和定义适用于本文件。

3.1

控制芯片 control chip

指汽车上能够独立运行并控制汽车系统部件的微控制器。

3.2

相关项 item

适用于GB/T 34590，实现整车层面功能或部分功能的系统或系统组合。

3.3

系统 system

一组至少与一个传感器、一个控制器和一个执行器相关联的组件或子系统。

注：相关的传感器或执行器可包含在系统中，也可存在于系统之外。

3.4

要素 element

系统、组件(硬件或软件)、硬件元器件或软件单元。

注1：当使用“软件要素”或“硬件要素”时，分别表示仅是软件的要素或硬件的要素。

注2：要素也可以是一个独立于环境的安全要素。

3.5

组件 component

由一个以上硬件元器件或一个到多个软件单元组成的逻辑上或技术上可分的非系统层面的要素。

示例：控制芯片。

注：组件是系统的一部分。

3.6

硬件元器件 hardware part

硬件组件在第一层级分解时的一部分。

示例：控制芯片的CPU、电阻、控制芯片的闪存阵列。

3.7

功能概念 functional concept

实现预期表现所需的各预期功能及其交互的定义。

注：功能概念是在概念阶段开发的。

3.8

功能安全 functional safety

不存在由电子电气系统的功能异常表现引起的危害而导致不合理的风险。

3.9

功能安全概念 functional safety concept

为了实现安全目标，定义功能安全要求及相关信息，并将要求分配到架构中的要素上，以及定义要素之间的必要交互。

3.10

功能安全要求 functional safety requirement

定义了独立于具体实现方式的安全行为,或独立于具体实现方式的安全措施,包括安全相关的属性。

注 1：功能安全要求可以是由安全相关的电子电气系统或基于其它技术的安全相关系统所执行的安全要求，目的是通过考虑确定的危害事件，使相关项达到或保持在安全状态。

注 2：功能安全要求的定义可独立于产品开发概念阶段中使用的技术。

注 3：安全相关的属性包括 ASIL 等级信息。

3.11

技术安全概念 technical safety concept

技术安全要求的定义，技术安全要求在系统要素间的分配，以及为系统层面功能安全提供依据的相关信息。

3.12

技术安全要求 technical safety requirement

为实现相关的功能安全要求而得出的要求。

注：得出的要求包括减轻失效所需的要求。

3.13

测试 testing

为验证相关项或要素满足定义的要求、探测其安全异常、确认要求适用于给定的环境和对其行为建立信心，而进行计划、准备、运行或演练的过程。

3.14

验证 verification

确定检查对象是否满足其特定要求。

3.15

系统性失效 systematic failure

以确定的方式与某个原因相关的失效，只有对设计或生产流程、操作规程、文档或其它相关因素进行变更后才可能排除这种失效。

3.16

系统性故障 systematic fault

以确定的方式显现失效的故障，只有通过使用流程或设计措施才有可能防止其发生。

3.17

汽车安全完整性等级 automotive safety integrity level；ASIL

四个等级中的一个等级，用于定义相关项或要素需要满足的GB/T 34590中的要求和安全措施，以避免不合理的风险，其中，D代表最高严格等级，A代表最低严格等级。

注：QM不是一个ASIL等级。

3.18

独立于环境的安全要素 safety element out of context；SEooC

不是在特定的相关项定义下开发的安全要素。

注：一个SEooC的安全要素可以是一个系统，系统组合，一个软件组件，一个软件单元，一个硬件组件，或一个硬件元器件。

3.19

故障容错时间间隔 fault tolerant time interval；FTTI

在安全机制未被激活情况下，从相关项内部故障发生到可能发生危害事件的最短时间间隔。

注 1：安全相关的时间间隔见图 1。

注 2：该最短时间间隔是通过评估所有危害事件得到的，其可以取决于危害的特征。

注 3：FTTI 与相关项的功能异常表现而引起的危害有关。FTTI 是源于该危害的安全目标的一个相关属性。

注 4：在容错时间间隔内，如果相关项保持在安全状态或过渡到安全状态或过渡到紧急运行，则表明安全机制及时对故障进行了处理。

注 5：危害事件的发生取决于存在的故障并且车辆处于故障可影响车辆行为的场景中。

注 6：虽然仅在相关项层面定义FTTI，但在要素层面可以定义最长故障处理时间间隔和故障处理后要求达到的状态，以支持功能安全概念。

注 7：当诊断测试时间间隔比故障探测时间间隔足够短时，故障探测时间间隔可包括多个诊断测试时间间隔用于消除错误。

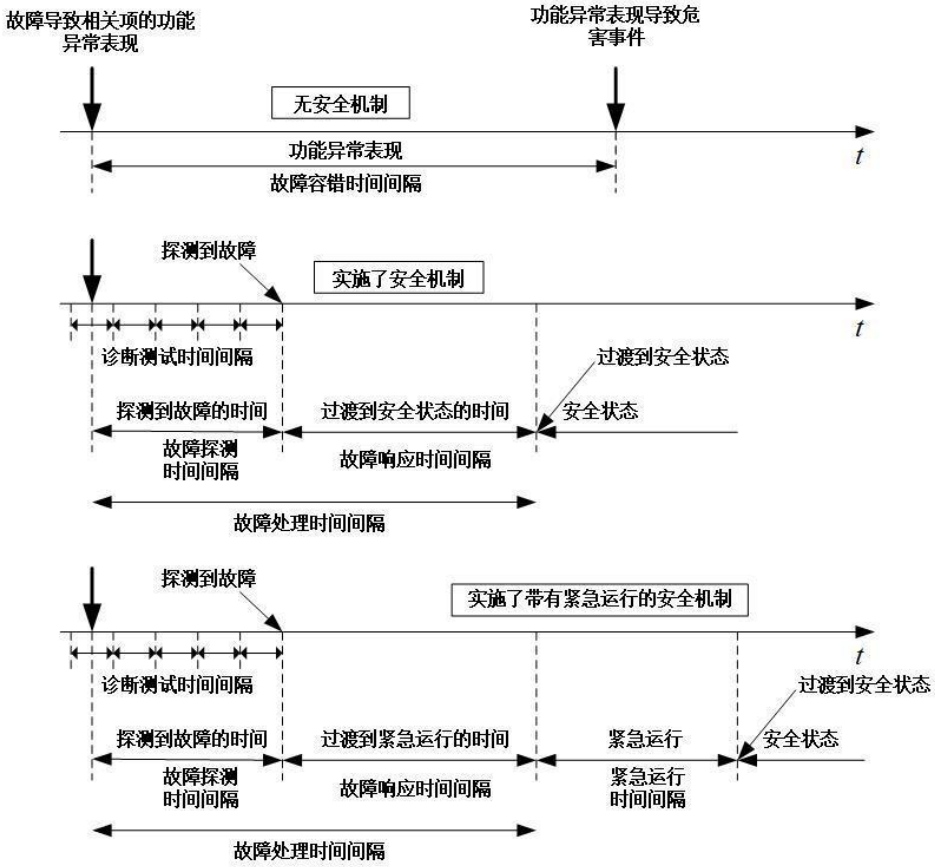

图 1 安全相关时间间隔

3.20

故障响应时间间隔 fault reaction time interval; FRTI

从探测到故障到进入安全状态或进入紧急运行的时间间隔。

3.21

故障处理时间间隔 fault handling time interval; FHTI

故障探测时间间隔和故障响应时间间隔的总和。

注：FHTI是安全机制的一种属性。

3.22

安全机制 safety mechanism

为保持预期功能或达到/保持某种安全状态，通过电气/电子系统的功能/要素或者其他技术手段所采取的技术措施，以探测并减轻、容许故障，或者控制、避免失效。

注 1：在相关项实施安全机制以避免故障导致单点失效和防止故障成为潜伏故障。

注 2：安全机制也可用于以下目的：

a) 能够使相关项过渡到或保持在安全状态；

b) 如同在功能安全概念中定义的，能够向驾驶员发出提醒以控制失效的影响。

3.23

失效模式 failure mode

要素或相关项未能提供预期行为的方式。

3.24

安全状态 safe state

相关项在失效的情况下，没有不合理风险的运行模式。

4 一般要求

除非特别说明，功能安全控制芯片所涉及到的流程开发等应符合GB/T 34590（适用部分）。 应通过符合功能安全标准的开发流程，保障不同 ASIL 等级控制芯片的系统性失效风险处于可接受范围内。

5 ASIL 等级指标技术要求

5.1 总则

ASIL等级指标要求适用范围仅限于控制芯片的随机硬件失效，本章中所提及的评估方法仅考虑由于芯片内部电路失效导致违反安全目标的情况。

按照类型划分，控制芯片的组成主要有六个部分：计算/逻辑控制单元、易失性/非易失性存储单元、片内/片外通信单元、电源管理单元、时钟管理单元、以及信号输入/输出控制单元。因此控制芯片ASIL等级技术要求的适用对象也为这六部分。

注1：控制芯片中若存在除上述六种类型以外的电路部分，也可参考本文中所描述的ASIL等级指标要求进行相关的评估活动。复位单元不单独考虑，而是分散到各个模块中进行分析。

注2：针对与控制芯片连接的其它器件，可以参考其它相关标准，例如针对电源管理芯片的技术要求和评估方法，可以参考《汽车电源管理芯片功能安全ASIL等级技术要求及评估方法》。

芯片使用方应根据自身功能安全需求及芯片使用场景评估上述控制芯片的六部分是否需部分或全部满足所分配的ASIL等级目标。

对于芯片外部环境或使用因素所导致的芯片失效场景，芯片使用方应根据芯片设计方提出的使用假设在系统级层面进行合理可靠的设计，同时应确保控制芯片的运行状态在芯片数据手册所规定的范围内。

5.2 控制芯片整体 ASIL 等级指标技术要求

5.2.1 指标依据

本章节要求适用于控制芯片ASIL等级目标为B，C和D的情况，应参照GB/T34590.5标准第8章及附录C中所描述的内容进行控制芯片硬件架构度量的评估，以及参照GB/T34590.5标准第9章9.4.2及附录F中所描述的内容进行控制芯片随机硬件失效导致违背安全目标的残余风险的评估。

相关方应结合控制芯片各个子模块和封装的失效率，失效模式以及安全机制诊断覆盖率，根据规定的评估方法及通过准则判定控制芯片是否满足目标ASIL等级指标。

注1：芯片设计阶段中，相关方主要为芯片设计方；芯片使用阶段中，相关方主要为芯片使用方。

注2：芯片使用过程中，芯片使用方应根据芯片设计方提供的各个子模块和封装的电路失效率，失效模式以及安全机制诊断覆盖率数据，并结合芯片的实际应用情况开展评估工作。

控制芯片针对自身随机硬件失效的有效性应满足目标ASIL等级所对应的硬件架构度量指标。

控制芯片中随机硬件失效导致违背安全目标的残余风险应满足目标ASIL等级所对应的量化指标。

针对控制芯片的评估过程及结果，相关方应根据GB/T 34590.8第9章中的要求进行验证评审，从而保证技术正确性及完整性。

5.2.2 指标要求

针对控制芯片ASIL等级目标为B，C和D的情况，全芯片的单点故障度量评估结果应满足表1中对应的指标要求。

表 1 控制芯片“单点故障度量”目标值

	ASIL B	ASIL C	ASIL D
单点故障度量	≥90%	≥97%	≥99%

针对控制芯片ASIL等级目标为B，C和D的情况，全芯片的潜伏故障度量评估结果应满足表2中对应的指标要求。

表 2 控制芯片“潜伏故障度量”目标值

	ASIL B	ASIL C	ASIL D
潜伏故障度量	≥60%	≥80%	≥90%

针对控制芯片ASIL等级目标为B，C和D的情况，全芯片随机硬件失效导致违背安全目标的残余风险应满足表3中对应的指标要求。

表 3 控制芯片“随机硬件失效”目标值

ASIL 等级	随机硬件失效目标值
D	$<10^{-8}\,h^{-1}$
C	$<10^{-7}\,h^{-1}$
B	$<10^{-7}\,h^{-1}$

注1：表1中“单点故障度量”目标值依据GB/T 34590.5标准中8.4.5条确定，表2中“潜伏故障度量”目标值依据GB/T 34590.5标准中8.4.6条确定；表3中“随机硬件失效”目标值依据GB/T 34590.5标准中9.4.2.1条确定。

注2：针对控制芯片是否满足表1/表2/表3中的目标值需求，一般通过GB/T 34590.5标准附录C以及本标准附录A的方式进行技术指标验证。

5.2.3 独立性要求

应分析控制芯片各个单元之间的相关失效，包括各层级模块间可能存在的共因失效和级联失效，并且评估其造成安全目标（或相关安全需求）违反的风险，以及如何制定应对的安全措施，从而在必要情况下，减轻此类风险。

在相关失效分析过程中，相关失效触发源可包括系统性失效，随机硬件失效和环境异常，可以按如下进行分类（允许有其它分类）：

—— 共用资源的故障；
—— 单个底层物理原因；
—— 环境故障；
—— 开发缺陷；
—— 生产制造缺陷；
—— 安装错误；

—— 维修错误。

对于每个相关故障应制定相关的安全措施，可能的安全措施分为：

—— 防止运行期间发生关联故障的措施；

—— 不能阻止关联故障的发生，但能防止造成安全目标违反的措施。

通过相关失效分析，进一步评估已有安全概念的潜在薄弱环节，并为满足独立性需求提供佐证。完成相关失效分析之后，应进行相应的评审和认可评审。

5.3 计算/逻辑控制单元的 ASIL 等级指标技术要求

5.3.1 指标依据

本章节要求适用于控制芯片计算/逻辑控制单元ASIL等级目标为B,C和D的情况,应参照GB/T34590.5标准第8章及附录C中所描述的内容进行计算/逻辑控制单元硬件架构度量的评估,以及参照GB/T34590.5标准第9章9.4.2及附录F中所描述的内容进行计算/逻辑控制单元随机硬件失效导致违背安全目标的残余风险的评估。

注：控制芯片中典型的计算/逻辑控制单元包含但不限于以下硬件组件：中央处理器、信号处理加速器、中断处理/路由单元、复位单元等。

相关方应结合计算/逻辑控制单元的数字电路失效率，失效模式以及安全机制诊断覆盖率，根据规定的评估方法及通过准则判定控制芯片计算/逻辑控制单元是否满足目标ASIL等级指标。

注1：芯片设计阶段中，相关方主要为芯片设计方；芯片使用阶段中，相关方主要为芯片使用方。

注2：芯片使用过程中，芯片使用方应根据芯片设计方提供的计算/逻辑控制单元的数字电路失效率，失效模式以及安全机制诊断覆盖率数据，并结合芯片的实际应用情况开展评估工作。

控制芯片计算/逻辑控制单元针对自身随机硬件失效的有效性应满足目标ASIL等级所对应的硬件架构度量指标。

控制芯片计算/逻辑控制单元中随机硬件失效导致违背安全目标的残余风险应满足目标ASIL等级所对应的量化指标。

针对控制芯片计算/逻辑控制单元的评估过程及结果，相关方应根据GB/T 34590.8第9章中的要求进行验证评审，从而保证技术正确性及完整性。

5.3.2 指标要求

针对控制芯片计算/逻辑控制单元ASIL等级目标为B，C和D的情况，计算/逻辑控制单元电路的单点故障度量评估结果应满足表4中对应的指标要求。

表 4 计算/逻辑控制单元“单点故障度量”目标值

	ASIL B	ASIL C	ASIL D
单点故障度量	≥90%	≥97%	≥99%

针对控制芯片计算/逻辑控制单元ASIL等级目标为B，C和D的情况，计算/逻辑控制单元电路的潜伏故障度量评估结果应满足表5中对应的指标要求。

表 5 计算/逻辑控制单元“潜伏故障度量”目标值

	ASIL B	ASIL C	ASIL D
潜伏故障度量	≥60%	≥80%	≥90%

针对控制芯片计算/逻辑控制单元ASIL等级目标为B，C和D的情况，计算/逻辑控制单元电路中随机硬件失效导致违背安全目标的残余风险应满足表6中对应的指标要求。

表 6 计算/逻辑控制单元“随机硬件失效”目标值

ASIL 等级	随机硬件失效目标值
D	＜10^{-8} h^{-1}
C	＜10^{-7} h^{-1}
B	＜10^{-7} h^{-1}

注1：表1中“单点故障度量”目标值依据GB/T 34590.5标准中8.4.5条确定，表2中“潜伏故障度量”目标值依据GB/T 34590.5标准中8.4.6条确定，表3中“随机硬件失效”目标值依据GB/T 34590.5标准中9.4.2.1条确定。

注2：针对芯片计算/逻辑控制单元是否满足表4/表5/表6中的目标值需求，一般通过GB/T 34590.5标准附录C以及本标准附录A的方式进行技术指标验证。

5.4 易失性/非易失性存储单元的 ASIL 等级指标技术要求

5.4.1 指标依据

本章节要求适用于控制芯片易失性/非易失性存储单元ASIL等级目标为B，C和D的情况，应参照GB/T34590.5标准第8章及附录C中所描述的内容进行易失性/非易失性存储单元硬件架构度量的评估，以及参照GB/T34590.5标准第9章9.4.2及附录F中所描述的内容进行易失性/非易失性存储单元随机硬件失效导致违背安全目标的残余风险的评估。

注1：控制芯片中典型的非易失性存储单元包含但不限于以下硬件组件：ROM、eFLASH、eFLASH控制单元、复位单元等。

注2：控制芯片中典型的易失性存储单元包含但不限于以下硬件组件：SRAM、SRAM控制单元、复位单元等。

相关方应结合易失性/非易失性存储单元中存储部分与数字逻辑电路的失效率，失效模式以及安全机制诊断覆盖率，根据规定的评估方法及通过准则判定控制芯片易失性/非易失性存储单元是否满足目标ASIL等级指标。

注1：芯片设计阶段中，相关方主要为芯片设计方；芯片使用阶段中，相关方主要为芯片使用方。

注2：芯片使用过程中，芯片使用方应根据芯片设计方提供的存储部分与数字逻辑电路失效率，失效模式以及安全机制诊断覆盖率数据，并结合芯片的实际应用情况开展评估工作。

控制芯片易失性/非易失性存储单元针对自身随机硬件失效的有效性应满足目标ASIL等级所对应的硬件架构度量指标。

控制芯片易失性/非易失性存储单元中随机硬件失效导致违背安全目标的残余风险应满足目标ASIL等级所对应的量化指标。

针对控制芯片易失性/非易失性存储单元的评估过程及结果，相关方应根据GB/T34590.8第9章中的要求进行验证评审，从而保证技术正确性及完整性。

5.4.2 指标要求

针对控制芯片易失性/非易失性存储单元ASIL等级目标为B，C和D的情况，易失性/非易失性存储单元电路的单点故障度量评估结果应满足表7中对应的指标要求。

表 7 易失性/非易失性存储单元“单点故障度量”目标值

	ASIL B	ASIL C	ASIL D
单点故障度量	≥90%	≥97%	≥99%

针对控制芯片易失性/非易失性存储单元ASIL等级目标为B，C和D的情况，易失性/非易失性存储单元电路的潜伏故障度量评估结果应满足表8中对应的指标要求。

表 8 易失性/非易失性存储单元“潜伏故障度量”目标值

	ASIL B	ASIL C	ASIL D
潜伏故障度量	≥60%	≥80%	≥90%

针对控制芯片易失性/非易失性存储单元ASIL等级目标为B，C和D的情况，易失性/非易失性存储单元电路中随机硬件失效导致违背安全目标的残余风险应满足表9中对应的指标要求。

表 9 易失性/非易失性存储单元“随机硬件失效”目标值

ASIL 等级	随机硬件失效目标值
D	$<10^{-8}\,h^{-1}$
C	$<10^{-7}\,h^{-1}$
B	$<10^{-7}\,h^{-1}$

注1：表4“单点故障度量”目标值依据GB/T 34590.5标准中8.4.5条确定，表5“潜伏故障度量”目标值依据GB/T 34590.5标准中8.4.6条确定，表6“随机硬件失效”目标值依据GB/T 34590.5标准中9.4.2.1条确定。

注2：针对芯片易失性/非易失性存储单元是否满足表7/表8/表9中的目标值需求，一般通过GB/T 34590.5标准附录C以及本标准附录A的方式进行技术指标验证。

5.5 片内/片外通信单元的 ASIL 等级指标技术要求

5.5.1 指标依据

本章节要求适用于控制芯片片内/片外通信单元ASIL等级目标为B,C和D的情况,应参照GB/T34590.5标准第8章及附录C中所描述的内容进行片内/片外通信单元硬件架构度量的评估,以及参照GB/T34590.5标准第9章9.4.2及附录F中所描述的内容进行片内/片外通信单元随机硬件失效导致违背安全目标的残余风险的评估。

注1：控制芯片中典型的片内通信单元包含但不限于以下硬件组件：内部总线互联、复位单元等。

注2：控制芯片中典型的片外通信单元包含但不限于以下硬件组件：CAN通信模块、SPI通信模块、以太网通信模块、复位单元等。

相关方应结合片内/片外通信单元的数字电路失效率，失效模式以及安全机制诊断覆盖率，根据规定的评估方法及通过准则判定控制芯片通信单元是否满足目标ASIL等级指标。

注1：芯片设计阶段中，相关方主要为芯片设计方；芯片使用阶段中，相关方主要为芯片使用方。

注2：芯片使用过程中，芯片使用方应根据芯片设计方提供的片内/片外通信单元的数字电路失效率，失效模式以及安全机制诊断覆盖率数据，并结合芯片的实际应用情况开展评估工作。

控制芯片通信单元针对自身随机硬件失效的有效性应满足目标ASIL等级所对应的硬件架构度量指标。

控制芯片通信单元中随机硬件失效导致违背安全目标的残余风险应满足目标ASIL等级所对应的量化指标。

针对控制芯片通信单元的评估过程及结果，相关方应根据GB/T34590.8第9章中的要求进行验证评审，从而保证技术正确性及完整性。

5.5.2 指标技术要求

针对控制芯片通信单元ASIL等级目标为B，C和D的情况，片内/片外通信单元电路的单点故障度量评估结果应满足表10中对应的指标技术要求。

表 10 片内/片外通信单元“单点故障度量”目标值

	ASIL B	ASIL C	ASIL D
单点故障度量	≥90%	≥97%	≥99%

针对控制芯片通信单元ASIL等级目标为B，C和D的情况，片内/片外通信单元电路的潜伏故障度量评估结果应满足表11中对应的指标技术要求。

表 11 片内/片外通信单元“潜伏故障度量”目标值

	ASIL B	ASIL C	ASIL D
潜伏故障度量	≥60%	≥80%	≥90%

针对控制芯片通信单元ASIL等级目标为B，C和D的情况，片内/片外通信单元电路中随机硬件失效导致违背安全目标的残余风险应满足表12中对应的指标技术要求。

表 12 片内/片外通信单元“随机硬件失效”目标值

ASIL 等级	随机硬件失效目标值
D	$<10^{-8}\,h^{-1}$
C	$<10^{-7}\,h^{-1}$
B	$<10^{-7}\,h^{-1}$

注1：表7中“单点故障度量”目标值依据GB/T 34590.5标准中8.4.5条确定；表8中“潜伏故障度量”目标值依据GB/T 34590.5标准中8.4.6条确定，表9“随机硬件失效”目标值依据GB/T 34590.5标准中9.4.2.1条确定。

注2：针对芯片通信单元是否满足表10/表11/表12中的目标值需求，一般通过GB/T 34590.5标准附录C以及本标准附录A的方式进行技术指标验证。

5.6 电源管理单元的 ASIL 等级指标技术要求

5.6.1 指标依据

本章节要求适用于控制芯片电源管理单元ASIL等级目标为B，C和D的情况，应参照GB/T34590.5标准第8章及附录C中所描述的内容进行电源管理单元硬件架构度量的评估，以及参照GB/T34590.5标准第9章9.4.2及附录F中所描述的内容进行电源管理单元随机硬件失效导致违背安全目标的残余风险的评估。

注：控制芯片中典型的电源管理单元包含但不限于以下硬件组件：线性稳压器、开关型稳压器、电源控制单元、复位单元等。

相关方应结合电源管理单元中数字逻辑电路与电源模拟电路的失效率，失效模式以及安全机制诊断覆盖率，根据规定的评估方法及通过准则判定控制芯片电源管理单元是否满足目标ASIL等级指标。

注1：芯片设计阶段中，相关方主要为芯片设计方；芯片使用阶段中，相关方主要为芯片使用方。

注2：芯片使用过程中，芯片使用方应根据芯片设计方提供的数字逻辑电路与电源模拟电路的失效率，失效模式以及安全机制诊断覆盖率数据，并结合芯片的实际应用情况开展评估工作。

控制芯片电源管理单元针对自身随机硬件失效的有效性应满足目标ASIL等级所对应的硬件架构度量指标。

控制芯片电源管理单元中随机硬件失效导致违背安全目标的残余风险应满足目标ASIL等级所对应的量化指标。

针对控制芯片电源管理单元的评估过程及结果，相关方应根据GB/T34590.8第9章中的要求进行验证评审，从而保证技术正确性及完整性。

5.6.2 指标要求

针对控制芯片电源管理单元ASIL等级目标为B，C和D的情况，电源管理单元电路的单点故障度量评估结果应满足表13中对应的指标要求。

表 13 电源管理单元“单点故障度量”目标值

	ASIL B	ASIL C	ASIL D
单点故障度量	≥90%	≥97%	≥99%

针对控制芯片电源管理单元ASIL等级目标为B，C和D的情况，电源管理单元电路的潜伏故障度量评估结果应满足表14中对应的指标要求。

表 14 电源管理单元“潜伏故障度量”目标值

	ASIL B	ASIL C	ASIL D
潜伏故障度量	≥60%	≥80%	≥90%

针对控制芯片电源管理单元ASIL等级目标为B，C和D的情况，电源管理单元电路中随机硬件失效导致违背安全目标的残余风险应满足表15中对应的指标要求。

表 15 电源管理单元“随机硬件失效”目标值

ASIL 等级	随机硬件失效目标值
D	$<10^{-8}\,h^{-1}$
C	$<10^{-7}\,h^{-1}$
B	$<10^{-7}\,h^{-1}$

注1：表10“单点故障度量”目标值依据GB/T 34590.5标准中8.4.5条确定，表11“潜伏故障度量”目标值依据GB/T 34590.5标准中8.4.6条确定，表12“随机硬件失效”目标值依据GB/T 34590.5标准中9.4.2.1条确定。

注2：针对芯片电源管理单元是否满足表13/表14/表15中的目标值需求，一般通过GB/T 34590.5标准附录C以及本标准附录A的方式进行技术指标验证。

5.7 时钟管理单元的 ASIL 等级技术要求

5.7.1 指标依据

本章节要求适用于控制芯片时钟管理单元ASIL等级目标为B，C和D的情况，应参照GB/T34590.5标准第8章及附录C中所描述的内容进行时钟管理单元硬件架构度量的评估，以及参照GB/T34590.5标准第9章9.4.2及附录F中所描述的内容进行时钟管理单元随机硬件失效导致违背安全目标的残余风险的评估。

注：控制芯片中典型的时钟管理单元包含但不限于以下硬件组件：锁相环、时钟控制单元、复位单元等。

相关方应结合时钟管理单元中数字逻辑电路与时钟模拟电路的失效率，失效模式以及安全机制诊断覆盖率，根据规定的评估方法及通过准则判定控制芯片时钟管理单元是否满足目标ASIL等级指标。

注1：芯片设计阶段中，相关方主要为芯片设计方；芯片使用阶段中，相关方主要为芯片使用方。

注2：芯片使用过程中，芯片使用方应根据芯片设计方提供的数字逻辑电路与时钟模拟电路的失效率，失效模式以及安全机制诊断覆盖率数据，并结合芯片的实际应用情况开展评估工作。

控制芯片时钟管理单元针对自身随机硬件失效的有效性应满足目标ASIL等级所对应的硬件架构度量指标。

控制芯片时钟管理单元中随机硬件失效导致违背安全目标的残余风险应满足目标ASIL等级所对应的量化指标。

针对控制芯片时钟管理单元的评估过程及结果，相关方应根据GB/T34590.8第9章中的要求进行验证评审，从而保证技术正确性及完整性。

5.7.2 指标要求

针对控制芯片时钟管理单元ASIL等级目标为B，C和D的情况，时钟管理单元电路的单点故障度量评估结果应满足表16中对应的指标要求。

表 16 时钟管理单元“单点故障度量”目标值

	ASIL B	ASIL C	ASIL D
单点故障度量	≥90%	≥97%	≥99%

针对控制芯片时钟管理单元ASIL等级目标为B，C和D的情况，时钟管理单元电路的潜伏故障度量评估结果应满足表17中对应的指标要求。

表 17 时钟管理单元“潜伏故障度量”目标值

	ASIL B	ASIL C	ASIL D
潜伏故障度量	≥60%	≥80%	≥90%

针对控制芯片时钟管理单元ASIL等级目标为B，C和D的情况，时钟管理单元电路中随机硬件失效导致违背安全目标的残余风险应满足表18中对应的指标要求。

表 18 时钟管理单元“随机硬件失效”目标值

ASIL 等级	随机硬件失效目标值
D	$<10^{-8}\,h^{-1}$
C	$<10^{-7}\,h^{-1}$
B	$<10^{-7}\,h^{-1}$

注1：表13“单点故障度量”目标值依据GB/T 34590.5标准中8.4.5条确定；表14“潜伏故障度量”目标值依据GB/T 34590.5标准中8.4.6条确定；表15“随机硬件失效”目标值依据GB/T 34590.5标准中9.4.2.1条确定。

注2：针对芯片时钟管理单元是否满足表16/表17/表18中的目标值需求，一般通过GB/T 34590.5标准附录C以及本标准附录A的方式进行技术指标验证。

5.8 信号输入/输出控制单元的 ASIL 等级指标技术要求

5.8.1 指标依据

本章节要求适用于控制芯片信号输入/输出控制单元ASIL等级目标为B，C和D的情况，应参照GB/T34590.5标准第8章及附录C中所描述的内容进行信号输入/输出控制单元硬件架构度量的评估，以及参照GB/T34590.5标准第9章9.4.2及附录F中所描述的内容进行信号输入/输出控制单元随机硬件失效导致违背安全目标的残余风险的评估。

注：控制芯片中典型的信号输入/输出控制单元包含但不限于以下硬件组件：ADC、DAC、IO接口、复位单元等。

相关方应结合信号输入/输出控制单元的数字逻辑与模拟部分电路失效率，失效模式以及安全机制诊断覆盖率，根据规定的评估方法及通过准则判定控制芯片信号输入/输出控制单元是否满足目标ASIL等级指标。

注1：芯片设计阶段中，相关方主要为芯片设计方；芯片使用阶段中，相关方主要为芯片使用方。

注2：芯片使用过程中，芯片使用方应根据芯片设计方提供的数字逻辑与模拟部分电路失效率，失效模式以及安全机制诊断覆盖率数据，并结合芯片的实际应用情况开展评估工作。

控制芯片信号输入/输出控制单元针对自身随机硬件失效的有效性应满足目标ASIL等级所对应的硬件架构度量指标。

控制芯片信号输入/输出控制单元中随机硬件失效导致违背安全目标的残余风险应满足目标ASIL等级所对应的量化指标。

针对控制芯片信号输入/输出控制单元的评估过程及结果，相关方应根据GB/T34590.8第9章中的要求进行验证评审，从而保证技术正确性及完整性。

5.8.2 指标要求

针对控制芯片信号输入/输出控制单元ASIL等级目标为B，C和D的情况，信号输入/输出控制单元电路的单点故障度量评估结果应满足表19中对应的指标要求。

表 19 信号输入/输出控制单元“单点故障度量”目标值

	ASIL B	ASIL C	ASIL D
单点故障度量	≥90%	≥97%	≥99%

针对控制芯片信号输入/输出控制单元ASIL等级目标为B，C和D的情况，信号输入/输出控制单元电路的潜伏故障度量评估结果应满足表20中对应的指标要求。

表 20 信号输入/输出控制单元“潜伏故障度量”目标值

	ASIL B	ASIL C	ASIL D
潜伏故障度量	≥60%	≥80%	≥90%

针对控制芯片信号输入/输出控制单元ASIL等级目标为B，C和D的情况，信号输入/输出控制单元电路中随机硬件失效导致违背安全目标的残余风险应满足表21中对应的指标要求。

表 21 信号输入/输出控制单元“随机硬件失效”目标值

ASIL 等级	随机硬件失效目标值
D	$<10^{-8}\,h^{-1}$
C	$<10^{-7}\,h^{-1}$
B	$<10^{-7}\,h^{-1}$

注1：表16“单点故障度量”目标值依据GB/T 34590.5标准中8.4.5条确定，表17“潜伏故障度量”目标值依据GB/T 34590.5标准中8.4.6条确定，表18“随机硬件失效”目标值依据GB/T 34590.5标准中9.4.2.1条确定。

注2：针对芯片信号输入/输出控制单元是否满足表19/表20/表21中的目标值需求，一般通过GB/T 34590.5标准附录C以及本标准附录A的方式进行技术指标验证。

6 ASIL 等级指标评估方法

6.1 总则

本章重点讨论如何通过评估方法，证明控制芯片符合功能安全 ASIL 等级指标要求。评估主要包括：电子元器件的基础失效率评估，失效模式及其分布率的评估，安全机制有效性及诊断覆盖率的评估。

6.2 控制芯片 ASIL 等级指标评估方法

6.2.1 评估目的

控制芯片包括裸片和封装，在评估各模块的指标之外，应评估控制芯片是否符合功能安全 ASIL 等级指标要求。

6.2.2 评估方法

6.2.2.1 控制芯片基础失效率评估和实施方法

评估和实施方法如下。

a) 评估方法

针对硬错误（Hard Error），基础失效率评估方法主要包含：

1) 使用业界公认的硬件元器件失效率数据，如根据 IEC/TR62380、IEC61709 或行业内等同标准中所描述的失效率计算公式推导得到；

注 1：工业标准中所提供的失效率数据一般都比较保守。

注 2：IEC/TR62380 计算公式计算的封装失效率包括硅片、外壳/封装（如壳体）以及连接点（如引脚）相关的故障。连接点与电路板之间的连接部分（如焊点）被视为电路板故障，通常由系统集成商在系统或元件层级的安全分析中予以考虑。

注 3：IEC/TR62380 封装失效率包含了封装内部的故障模式（包括裸片与引线框架之间的连接等），但同时也包含了封装连接点与电路板之间连接（即焊点）相关的故障率，这部分焊点故障率约占整体封装失效率的 20%。因此，芯片设计方可采用 $\lambda_{package}$ 值的 80%进行计算。

注 4：在业界同类方法中，有不同于 IEC/TR62380 的封装失效率的计算模式，也可以被采用。

2) 使用现场反馈或测试的统计数据；

3) 使用工程方法形成的专家判断，如现场经验、测试、可靠性分析等，具体方法参照 b）实施方法中的步骤。

b) 实施方法

通过加速寿命试验，可以有效地进行控制芯片基础失效率的测试。加速寿命试验的具体实施方法，具体可以参考国际国内相关标准。

当实施加速寿命试验进行失效率测量时，为了使寿命测试中的温度修正到最大运行温度，需要启用加速因子。该计算使用了阿伦尼乌斯方程，其中涉及到的活化能值建议通过评估和验证方式获取。

以样本中得到的故障数量作为输入，参与到 x 2分布（卡方分布）函数计算中，并考虑所需的置信度水平，从而获得在整个测试群体中可能发生的总故障数量。

针对软错误（Soft Error），基础失效率应依据国际国内相关标准中要求的测试方法来获得。

6.2.2.2 控制芯片失效模式及分布率评估和实施方法

评估和实施方法如下:

a) 裸片部分失效模式和分布率评估方法可参考 6.3-6.8 章节控制芯片各部分的方法。

b) 封装部分的失效模式和分布率评估的方法

基于 6.2.2.1 中得到的封装失效率，对于与安全相关的引脚，可以使用每个引脚的失效率来完

成失效率的分配，该失效率是通过将封装失效率分配给封装的总引脚数所得到的。

封装部分的失效模式一般包括：短路到地，短路到电源，开路，短路到相邻引脚。基于以上失效模式，并根据实际芯片设计分析得到。

注1：失效模式需根据芯片实际情况进行删减或补充。

封装部分的失效分布率评估,可根据现场反馈或测试的统计数据，若无法获得足够数据以计算符合精度要求的分布,则将故障率平均分配至各故障模式;或由专家提供附有相关论证的专业判断。

注2：可采用引脚等概率假设，但该假设并非适用于所有情况。

注3：在球栅阵列封装中，某些位置的故障分布概率可能高于其他位置。

6.2.2.3 控制芯片安全机制有效性及诊断覆盖率评估和实施方法

评估和实施方法如下：

a) 评估方法

评估方法如下：

1) 使用功能安全国际标准中的诊断覆盖率信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型安全机制诊断覆盖率；

2) 使用专家经验或根据安全机制设计原理进行数学推导得到。

3) 使用验证工具进行故障注入并根据测试结果计算得到，具体方法参照 b）实施方法中的步骤。

注：控制芯片的故障注入示例参考附录 C。

b) 实施方法

测试用例的实施，主要是针对控制芯片安全机制的有效性，测试实施的主要步骤包括（但不限于）：

1）使能安全机制；

2）选取故障点（实施故障注入的位置）以及诊断点（观察安全机制反应的位置）；

3）在选择的位置注入特定类型的故障，观测安全机制的动作和性能参数；

注1：注入特定类型的故障主要是指被测试项的物理故障模型，如Stuck at 0/1,floating等。

注2：安全机制的动作是指探测故障和处理故障，其中处理故障包括发出告警信号，置位相关故障状态位等。

注3：安全机制的性能参数是指故障探测时间间隔，故障响应时间间隔，安全机制的诊断覆盖率等。

4）记录测试中获取的信息和数据，确定被测试项的定性结果（安全机制的有效性）和定量结果（安全机制的诊断覆盖率）。

——在被测试项的定性结果方面，注入故障后，观测在一段时间内，安全机制能否正确处理故障，如发出告警信号，置位相关故障状态位等。

——在被测试项的定量结果方面，统计要素故障注入后，获取安全机制的故障探测时间间隔；故障响应时间间隔；以及安全机制的诊断覆盖率。

6.3 计算/逻辑控制单元的 ASIL 等级指标评估方法

6.3.1 评估目的

计算/逻辑控制单元是控制芯片执行逻辑运算和处理数据的关键，应评估计算/逻辑控制单元是否符合功能安全 ASIL 等级指标要求。

6.3.2 评估方法

6.3.2.1 计算/逻辑控制单元晶体管基础失效率评估和实施方法

评估和实施方法如下。

针对硬错误，基础失效率评估方法主要包含：

1) 使用业界公认的硬件元器件失效率数据，如根据 IEC/TR62380、IEC61709 或行业内等同标准中所描述的失效率计算公式推导得到；

注 1：工业标准中所提供的失效率数据一般都比较保守。

2) 使用现场反馈或测试的统计数据；

3) 使用工程方法形成的专家判断，如现场经验、测试、可靠性分析等，具体方法如下。

——通过加速寿命试验，可以有效地进行计算/逻辑控制单元晶体管基础失效率的测试。加速寿命试验的具体实施方法，具体可以参考国际国内相关标准。

——当实施加速寿命试验进行失效率测量时，为了使寿命测试中的温度修正到最大运行温度，需要启用加速因子。该计算使用了阿伦尼乌斯方程，其中涉及到的活化能值建议通过评估和验证方式获取。

——以样本中得到的故障数量作为输入，参与到$\chi 2$ 分布（卡方分布）函数计算中，并考虑所需的置信度水平，从而获得在整个测试群体中可能发生的总故障数量。

——针对软错误，基础失效率应依据国际国内相关标准中要求的测试方法来获得。

6.3.2.2 计算/逻辑控制单元失效模式及分布率评估方法

评估和实施方法如下。

a) 评估方法

评估方法如下：

1) 使用功能安全国际标准中的失效模式信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型电路失效模式；

注 1：功能安全标准中所列举的典型电路失效模式需根据芯片实际情况进行删减或补充。

注 2：控制芯片计算/逻辑控制单元的典型失效模式示例参考附录 B。

2) 使用专家判断或根据芯片电路设计原理分析得到。

3) 使用验证工具进行故障注入或统计芯片测试过程中所观察到的失效模式,具体方法参照 b）实施方法中的步骤。

b) 实施方法

在计算/逻辑控制单元的测试中，将测试功能电路的功能失效作为主要关注点，在被测试电路的特定位置注入所需的故障模型和失效模式，以表征被测试电路的功能失效。

具体的测试实施步骤包括（但不限于）：

1）选取故障点（实施故障注入的位置）及观测点（观察故障影响的位置）；

2）在选择的位置注入特定类型的故障，观测故障影响；

示例：如在中断处理/路由单元的中断生成电路注入故障，表征中断生成电路的中断请求丢失故障。

注：故障影响是指要素的失效对相关性的影响为安全故障，单点故障，或潜伏故障。

3）分析测试中获取的信息和数据，确定被测试项的定性结果（失效模式及影响）和定量结果（失效模式分布率）。

——在被测试项的定性结果方面，列出要素每种失效模式类型的影响。

——在被测试项的定量结果方面，通过故障注入遍历所有的要素后，统计各类型失效模式的发生次数，计算各类型失效模式发生的比例。

注：失效模式分布是指各类型失效模式发生的比例。

6.3.2.3 计算/逻辑控制单元安全机制有效性及诊断覆盖率评估和实施方法

评估和实施方法如下.

a) 评估方法

评估方法如下：

1) 使用功能安全国际标准中的诊断覆盖率信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型安全机制诊断覆盖率；

2) 使用专家经验或根据安全机制设计原理进行数学推导得到。

3) 使用验证工具进行故障注入并根据测试结果计算得到，具体方法参照 b）实施方法中的步骤。

注：控制芯片计算/逻辑控制单元的故障注入示例参考附录 C。

b) 实施方法

测试用例的实施，主要是针对计算/逻辑控制单元安全机制的有效性，测试实施的主要步骤包括（但不限于）：

1）使能安全机制；

2）选取故障点（实施故障注入的位置）以及诊断点（观察安全机制反应的位置）；

3）在选择的位置注入特定类型的故障，观测安全机制的动作和性能参数；

注1：注入特定类型的故障主要是指被测试项的物理故障模型，如Stuck at 0/1,floating等。

注2：安全机制的动作是指探测故障和处理故障，其中处理故障包括发出告警信号，置位相关故障状态位等。

注3：安全机制的性能参数是指故障探测时间间隔，故障响应时间间隔，安全机制的诊断覆盖率等。

4）记录测试中获取的信息和数据，确定被测试项的定性结果（安全机制的有效性）和定量结果（安全机制的诊断覆盖率）。

——在被测试项的定性结果方面，注入故障后，观测在一段时间内，安全机制能否正确处理故障，如发出告警信号，置位相关故障状态位等。

——在被测试项的定量结果方面，统计要素故障注入后，获取安全机制的故障探测时间间隔；故障响应时间间隔；以及安全机制的诊断覆盖率。

6.4 易失性/非易失性存储单元的 ASIL 等级指标评估方法

6.4.1 评估目的

易失性/非易失性存储单元的主要功能是存储数据和程序代码，以便在需要时能够快速读取和写入。应评估存储单元是否符合功能安全 ASIL 等级指标要求。

6.4.2 评估方法

6.4.2.1 易失性/非易失性存储单元数字逻辑电路晶体管和存储部分电子元器件基础失效率评估和实施方法

评估和实施方法如下。

针对硬错误，基础失效率评估方法主要包含：

1) 使用业界公认的硬件元器件失效率数据，如根据 IEC/TR62380、IEC61709 或行业内等同标准中所描述的失效率计算公式推导得到；

注 1: 工业标准中所提供的失效率数据一般都比较保守。

2) 使用现场反馈或测试的统计数据；

3) 使用工程方法形成的专家判断，如现场经验、测试、可靠性分析等，具体方法如下。

注2：针对存储部分与数字逻辑电路失效率的计算应基于易失性/非易失性存储单元的实际应用情况进行综合考虑，包含但不限于如下因素：物理电路类型、网表综合结果、芯片制程工艺、芯片使用工况等。

——通过加速寿命试验，可以有效地进行存储单元数字逻辑电路晶体管和存储部分电子元器件基础失效率的测试。加速寿命试验的具体实施方法，具体可以参考国际国内相关标准。

——当实施加速寿命试验进行失效率测量时，为了使寿命测试中的温度修正到最大运行温度，需要启用加速因子。该计算使用了阿伦尼乌斯方程，其中涉及到的活化能值建议通过评估和验证方式获取。

——以样本中得到的故障数量作为输入，参与到χ2 分布（卡方分布）函数计算中，并考虑所需的置信度水平，从而获得在整个测试群体中可能发生的总故障数量。

——针对软错误，基础失效率应依据国际国内相关标准中要求的测试方法来获得。

6.4.2.2 易失性/非易失性存储单元失效模式及分布率评估和实施方法

评估和实施方法如下。

a) 评估方法

评估方法如下：

1) 使用功能安全国际标准中的失效模式信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型电路失效模式；

注 1：功能安全标准中所列举的典型电路失效模式需根据芯片实际情况进行删减或补充

注 2：控制芯片易失性/非易失性存储单元的典型失效模式示例参考附录 B。

2) 使用专家判断或根据芯片电路设计原理分析得到；

3) 使用验证工具进行故障注入或统计芯片测试过程中所观察到的失效模式，具体方法参照 b）实施方法中的步骤。

注：控制芯片易失性/非易失性存储单元的故障注入示例参考附录 C。

b) 实施方法

在易失性/非易失性存储单元的测试中，将测试功能电路的功能失效作为主要关注点，在被测试电路的特定位置注入所需的故障模型和失效模式，以表征被测试电路的功能失效。测试实施的主要步骤包括（但不限于）：

1) 选取故障点（实施故障注入的位置）及观测点（观察故障影响的位置）；

2) 在选择的位置注入特定类型的故障，观测故障影响；

示例：如在存储单元的寻址逻辑电路注入故障，表征存储单元的寻址故障。

注：故障影响是指要素的失效对相关性的影响为安全故障，单点故障，或潜伏故障。

3) 分析测试中获取的信息和数据，确定被测试项的定性结果（失效模式及影响）和定量结果（失效模式分布率）。

——在被测试项的定性结果方面，列出要素每种失效模式类型的影响。

——在被测试项的定量结果方面，通过故障注入遍历所有的要素后，统计被测试项失效模式的发生次数，计算各类型失效模式发生的比例。

注：失效模式分布是指被测试项各失效模式发生的比例。

6.4.2.3 易失性/非易失性存储单元安全机制有效性及诊断覆盖率评估方法

评估和实施方法如下。

a) 评估方法

评估方法如下：

1) 使用功能安全国际标准中的诊断覆盖率信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型安全机制诊断覆盖率；

2）使用专家经验或根据安全机制设计原理进行数学推导得到；

3）使用验证工具进行故障注入并根据测试结果计算得到，具体方法参照 b）实施方法中的步骤。

注 1：控制芯片易失性/非易失性存储单元的故障注入示例参考附录 C。

注 2:针对控制芯片易失性/非易失性存储单元的故障注入应考虑存储部分与数字逻辑电路集成后的测试环境。

b) 实施方法

测试用例的实施，主要是针对易失性/非易失性存储单元安全机制的有效性，测试实施的主要步骤包括（但不限于）：

1）使能相关测试项的安全机制；

2）选取故障点（实施故障注入的位置）以及诊断点（观察安全机制反应的位置）；

3）在选择的位置注入特定类型的故障，观测安全机制的动作和性能参数；

注1：注入特定类型的故障主要是指被测试项的物理故障模型，如Stuck at 0/1,floating等。

注2：安全机制的动作是指探测故障和处理故障，其中处理故障包括发出告警信号，置位相关故障状态位等。

注3：安全机制的性能参数是指故障探测时间间隔，故障响应时间间隔，安全机制的诊断覆盖率等。

4）记录测试中获取的信息和数据，确定被测试项的定性结果（安全机制的有效性）和定量结果（安全机制的诊断覆盖率）。

——在被测试项的定性结果方面，注入故障后，观测在一段时间内，安全机制能否正确处理故障，如发出告警信号，置位相关故障状态位等。

——在被测试项的定量结果方面，统计要素故障注入后，获取安全机制的故障探测时间间隔；故障响应时间间隔；以及安全机制的诊断覆盖率。

6.5 片内/片外通信单元的 ASIL 等级指标评估方法

6.5.1 评估目的

片内/片外通信单元是控制芯片进行片内/片外进行数据交互通信的关键，应评估片内/片外通信单元是否符合功能安全 ASIL 等级指标要求。

6.5.2 评估方法

6.5.2.1 片内/片外通信单元晶体管基础失效率评估和实施方法

评估和实施方法如下。

针对硬错误，基础失效率评估方法主要包含：

1）使用业界公认的硬件元器件失效率数据，如根据 IEC/TR62380、IEC61709 或行业内等同标准中所描述的失效率计算公式推导得到；

注 1: 工业标准中所提供的失效率数据一般都比较保守。

2）使用现场反馈或测试的统计数据；

3）使用工程方法形成的专家判断，如现场经验、测试、可靠性分析等，具体方法如下。

注2：针对数字电路失效率的计算应基于片内/片外通信单元的实际应用情况进行综合考虑，包含但不限于如下因素：物理电路类型、网表综合结果、芯片制程工艺、芯片使用工况等。

——通过加速寿命试验，可以有效地进行片内/片外通信单元晶体管基础失效率的测试。加速寿命试验的具体实施方法，具体可以参考国际国内相关标准。

——当实施加速寿命试验进行失效率测量时，为了使寿命测试中的温度修正到最大运行温度，需要启用加速因子。该计算使用了阿伦尼乌斯方程，其中涉及到的活化能值建议通过评估和验证方式获取。

——以样本中得到的故障数量作为输入，参与到 x 2分布（卡方分布）函数计算中，并考虑所需的置信度水平，从而获得在整个测试群体中可能发生的总故障数量。

——针对软错误，基础失效率应依据国际国内相关标准中要求的测试方法来获得。

6.5.2.2 片内/片外通信单元失效模式及分布率评估和实施方法

评估和实施方法如下。

a) 评估方法

评估方法如下：

1) 使用功能安全国际标准中的失效模式信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型电路失效模式；

注 1：功能安全标准中所列举的典型电路失效模式需根据芯片实际情况进行删减或补充。

注 2：控制芯片通信单元的典型失效模式示例参考附录 B。

2) 使用专家判断或根据芯片电路设计原理分析得到；

3) 使用验证工具进行故障注入或统计芯片测试过程中所观察到的失效模式，具体方法参照 b）实施方法中的步骤。

注：控制芯片通信单元的故障注入示例参考附录 C。

b) 实施方法

在片内/片外通信单元的测试中，将测试功能电路的功能失效作为主要关注点，在被测试电路的特定位置注入所需的故障模型和失效模式，以表征被测试电路的功能失效。

具体的测试实施步骤包括（但不限于）：

1）选取故障点（实施故障注入的位置）及观测点（观察故障影响的位置）；

2）在选择的位置注入特定类型的故障，观测故障影响；

示例：如在片内/片外通信单元的消息发出端注入故障，表征片内/片外通信单元的消息发出电路故障。

注：故障影响是指要素的失效对相关性的影响为安全故障，单点故障，或潜伏故障。

3）分析测试中获取的信息和数据，确定被测试项的定性结果（失效模式及影响）和定量结果（失效模式分布率）。

——在被测试项的定性结果方面，列出要素每种失效模式类型的影响。

——在被测试项的定量结果方面，通过故障注入遍历所有的要素后，统计各类型失效模式的发生次数，计算各类型失效模式发生的比例。

注：失效模式分布是指各类型失效模式发生的比例。

6.5.2.3 片内/片外通信单元安全机制有效性及诊断覆盖率评估和实施方法

评估和实施方法如下。

a) 评估方法

评估方法如下：

1) 使用功能安全国际标准中的诊断覆盖率信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型安全机制诊断覆盖率；

2) 使用专家经验或根据安全机制设计原理进行数学推导得到；

3) 使用验证工具进行故障注入并根据测试结果计算得到，具体方法参照 b）实施方法中的步骤。

注：控制芯片通信单元的故障注入示例参考附录 C。

b) 实施方法

测试用例的实施，主要是针对片内/片外通信单元安全机制的有效性，测试实施的主要步骤包

括（但不限于）：

1）使能安全机制；

2）选取故障点（实施故障注入的位置）以及诊断点（观察安全机制反应的位置）；

3）在选择的位置注入特定类型的故障，观测安全机制的动作和性能参数；

注1：注入特定类型的故障主要是指被测试项的物理故障模型，如Stuck at 0/1,floating等。

注2：安全机制的动作是指探测故障和处理故障，其中处理故障包括发出告警信号，置位相关故障状态位等。

注3：安全机制的性能参数是指故障探测时间间隔，故障响应时间间隔，安全机制的诊断覆盖率等。

4）记录测试中获取的信息和数据，确定被测试项的定性结果（安全机制的有效性）和定量结果（安全机制的诊断覆盖率）。

——在被测试项的定性结果方面，注入故障后，观测在一段时间内，安全机制能否正确处理故障，如发出告警信号，置位相关故障状态位等。

——在被测试项的定量结果方面，统计要素故障注入后，获取安全机制的故障探测时间间隔；故障响应时间间隔；以及安全机制的诊断覆盖率。

6.6 电源管理单元的ASIL等级指标评估方法

6.6.1 评估目的

控制芯片电源管理单元的主要功能是提供稳定符合预期的供电，其组成包括数字逻辑电路和电源模拟电路。应评估电源管理单元的数字逻辑电路和电源模拟电路是否符合功能安全 ASIL 等级指标要求。

6.6.2 评估方法

6.6.2.1 电源管理单元数字逻辑电路晶体管和电源模拟电路电子元器件基础失效率评估和实施方法

针对电源管理单元中数字逻辑电路、晶体管及电源模拟电路等电子元器件的硬错误，其基础失效率评估和实施可采用以下方法：

a) 使用业界公认的硬件元器件失效率数据，如根据 IEC/TR62380、IEC61709 或行业内等同标准中所描述的失效率计算公式推导得到；

注 1: 工业标准中所提供的失效率数据通常较为保守。

b) 使用现场反馈或测试的统计数据；

c) 使用工程方法形成的专家判断，如现场经验、测试、可靠性分析等，具体方法如下。

注2：针对数字逻辑电路与电源模拟电路失效率的计算应基于电源管理单元的实际应用情况进行综合考虑，包含但不限于如下因素：物理电路类型、网表综合结果、芯片制程工艺、芯片使用工况等。

——通过加速寿命试验，可以有效地进行数字逻辑电路晶体管和电源模拟电路电子元器件基础失效率的测试。加速寿命试验的具体实施方法，具体可以参考国际国内相关标准。

——当实施加速寿命试验进行失效率测量时，为了使寿命测试中的温度修正到最大运行温度，需要启用加速因子。该计算使用了阿伦尼乌斯方程，其中涉及到的活化能值建议通过评估和验证方式获取。

——以样本中得到的故障数量作为输入，参与到$\chi 2$分布（卡方分布）函数计算中，并考虑所需的置信度水平，从而获得在整个测试群体中可能发生的总故障数量。

——针对软错误，基础失效率应依据国际国内相关标准中要求的测试方法来获得。

6.6.2.2 电源管理单元数字逻辑电路和电源模拟电路失效模式及分布率评估和实施方法

评估和实施方法如下。

a) 评估方法

评估方法如下：

1) 使用功能安全国际标准中的失效模式信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型电路失效模式；

注 1：功能安全标准中所列举的典型电路失效模式需根据芯片实际情况进行删减或补充

注 2：控制芯片电源管理单元的典型失效模式示例参考附录 B。

2) 使用专家判断或根据芯片电路设计原理分析得到；

3) 使用验证工具进行故障注入或统计芯片测试过程中所观察到的失效模式，具体方法参照 b）实施方法中的步骤。

注 1：控制芯片电源管理单元的故障注入示例参考附录 C。

注 2：针对控制芯片电源管理单元的故障注入应考虑电源模拟电路与数字逻辑电路集成后的测试环境。

b) 实施方法

在电源管理单元的测试中，将测试功能电路的功能失效作为主要关注点，在被测试电路的特定位置注入所需的故障模型和失效模式，以表征被测试电路的功能失效。

测试实施的主要步骤包括（但不限于）：

1）选取故障点（实施故障注入的位置）及观测点（观察故障影响的位置）；

2）在选择的位置注入特定类型的故障，观测故障影响；

示例：如在电源管理单元的电压控制单元注入故障，表征电源管理单元的供电故障。

注：故障影响是指要素的失效对相关性的影响为安全故障，单点故障，或潜伏故障。

3）分析测试中获取的信息和数据，确定被测试项的定性结果（失效模式及影响）和定量结果（失效模式分布率）。

——在被测试项的定性结果方面，列出要素每种失效模式类型的影响。

——在被测试项的定量结果方面，统计要素故障注入后，被测试项失效模式的发生次数，计算各类型失效模式发生的比例。

注：失效模式分布是指被测试项各失效模式发生的比例。

6.6.2.3 电源管理单元安全机制有效性及诊断覆盖率评估和实施方法

评估和实施方法如下。

a) 评估方法

评估方法如下：

1)使用功能安全国际标准中的诊断覆盖率信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型安全机制诊断覆盖率；

2)使用专家经验或根据安全机制设计原理进行数学推导得到；

3)使用验证工具进行故障注入并根据测试结果计算得到，具体方法参照 b)实施方法中的步骤。

注：控制芯片电源管理单元的故障注入示例参考附录 C。

b) 实施方法

测试用例的实施，主要是针对数字逻辑电路和模拟电路安全机制的有效性，测试实施的主要步骤包括（但不限于）：

1）使能相关测试项的安全机制；

2）选取故障点（实施故障注入的位置）以及诊断点（观察安全机制反应的位置）；

3）在选择的位置注入特定类型的故障，观测安全机制的动作和性能参数；

注1：注入特定类型的故障主要是指被测试项的物理故障模型，如Stuck at 0/1,floating等。

注2：安全机制的动作是指探测故障和处理故障，其中处理故障包括发出告警信号，置位相关故障状态位等。

注3：安全机制的性能参数是指故障探测时间间隔，故障响应时间间隔，安全机制的诊断覆盖率等。

4）记录测试中获取的信息和数据，确定被测试项的定性结果（安全机制的有效性）和定量结果（安全机制的诊断覆盖率）。

——在被测试项的定性结果方面，注入故障后，观测在一段时间内，安全机制能否正确处理故障，如发出告警信号，置位相关故障状态位等。

——在被测试项的定量结果方面，统计要素故障注入后，获取安全机制的故障探测时间间隔；故障响应时间间隔；以及安全机制的诊断覆盖率。

6.7 时钟管理单元的 ASIL 等级指标评估方法

6.7.1 评估目的

控制芯片时钟管理单元的主要功能是提供稳定符合预期的时钟信号，其组成包括数字逻辑电路和时钟模拟电路。应评估时钟管理单元的数字逻辑电路和时钟模拟电路是否符合功能安全 ASIL 等级指标要求。

6.7.2 评估方法

6.7.2.1 时钟管理单元数字逻辑电路晶体管和模拟电路电子元器件基础失效率评估和实施方法

评估和实施方法如下：

针对硬错误，基础失效率评估方法主要包含：

1） 使用业界公认的硬件元器件失效率数据，如根据 IEC/TR62380、IEC61709 或行业内等同标准中所描述的失效率计算公式推导得到；

注 1：工业标准中所提供的失效率数据一般都比较保守。

2） 使用现场反馈或测试的统计数据；

3） 使用工程方法形成的专家判断，如现场经验、测试、可靠性分析等，具体方法如下。

注 2：针对数字逻辑电路与时钟模拟电路失效率的计算应基于时钟管理单元的实际应用情况进行综合考虑，包含但不限于如下因素：物理电路类型、网表综合结果、芯片制程工艺、芯片使用工况等。

——通过加速寿命试验，可以有效地进行数字逻辑电路晶体管和时钟模拟电路电子元器件基础失效率的测试。加速寿命试验的具体实施方法，具体可以参考国际国内相关标准。

——当实施加速寿命试验进行失效率测量时，为了使寿命测试中的温度修正到最大运行温度，需要启用加速因子。该计算使用了阿伦尼乌斯方程，其中涉及到的活化能值建议通过评估和验证方式获取。

——以样本中得到的故障数量作为输入，参与到 x 2 分布（卡方分布）函数计算中，并考虑所需的置信度水平，从而获得在整个测试群体中可能发生的总故障数量。

——针对软错误，基础失效率应依据国际国内相关标准中要求的测试方法来获得。

6.7.2.2 时钟管理单元数字逻辑电路和时钟模拟电路失效模式及分布率评估方法

评估和实施方法如下。

a)评估方法

评估方法如下：

1)使用功能安全国际标准中的失效模式信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型电路失效模式；

注 1：功能安全标准中所列举的典型电路失效模式需根据芯片实际情况进行删减或补充

注 2：控制芯片时钟管理单元的典型失效模式示例参考附录 B。

2)使用专家判断或根据芯片电路设计原理分析得到；

3)使用验证工具进行故障注入或统计芯片测试过程中所观察到的失效模式，具体方法参照 b）实施方法中的步骤。

注 1：控制芯片时钟管理单元的故障注入示例参考附录 C。

注 2：针对控制芯片时钟管理单元的故障注入应考虑时钟模拟电路与数字逻辑电路集成后的测试环境。

b）实施方法

在时钟管理单元的测试中，将测试功能电路的功能失效作为主要关注点，在被测试电路的特定位置注入所需的故障模型和失效模式，以表征被测试电路的功能失效。

测试实施的主要步骤包括（但不限于）：

1）选取故障点（实施故障注入的位置）及观测点（观察故障影响的位置）；

2）在选择的位置注入特定类型的故障，观测故障影响；

示例：如在时钟管理单元的锁相环控制电路注入故障，表征时钟管理单元的锁相环故障。

注：故障影响是指要素的失效对相关性的影响为安全故障，单点故障，或潜伏故障。

3）分析测试中获取的信息和数据，确定被测试项的定性结果（失效模式及影响）和定量结果（失效模式分布率）。

——在被测试项的定性结果方面，列出要素每种失效模式类型的影响。

——在被测试项的定量结果方面，统计要素故障注入后，被测试项失效模式的发生次数，计算各类型失效模式发生的比例。

注：失效模式分布是指被测试项各失效模式发生的比例。

6.7.2.3 时钟管理单元安全机制有效性及诊断覆盖率评估和实施方法

评估和实施方法如下。

a）评估方法

评估方法如下：

1)使用功能安全国际标准中的诊断覆盖率信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型安全机制诊断覆盖率；

2)使用专家经验或根据安全机制设计原理进行数学推导得到；

3)使用验证工具进行故障注入并根据测试结果计算得到，具体方法参照 b）实施方法中的步骤。

注：控制芯片时钟管理单元的故障注入示例参考附录 C。

b）实施方法

测试用例的实施，主要是针对数字逻辑电路和模拟电路安全机制的有效性，测试实施的主要步骤包括（但不限于）：

1）使能相关测试项的安全机制；

2）选取故障点（实施故障注入的位置）以及诊断点（观察安全机制反应的位置）；

3）在选择的位置注入特定类型的故障，观测安全机制的动作和性能参数；

注1：注入特定类型的故障主要是指被测试项的物理故障模型，如Stuck at 0/1,floating等。

注2：安全机制的动作是指探测故障和处理故障，其中处理故障包括发出告警信号，置位相关故障状态位等。

注3：安全机制的性能参数是指故障探测时间间隔，故障响应时间间隔，安全机制的诊断覆盖率等。

4）记录测试中获取的信息和数据，确定被测试项的定性结果（安全机制的有效性）和定量结果（安全机制的诊断覆盖率）。

——在被测试项的定性结果方面，注入故障后，观测在一段时间内，安全机制能否正确处理故障，如发出告警信号，置位相关故障状态位等。

——在被测试项的定量结果方面，统计要素故障注入后，获取安全机制的故障探测时间间隔；故障响应时间间隔；以及安全机制的诊断覆盖率。

6.8 信号输入/输出控制单元的 ASIL 等级指标评估方法

6.8.1 评估目的

控制芯片信号输入/输出控制单元的主要功能是提供信号的数模、模数转换以及输入输出接口，其组成包括数字逻辑电路和模拟电路。应评估输入/输出控制单元的数字逻辑电路和模拟电路是否符合功能安全 ASIL 等级指标要求。

6.8.2 评估方法

6.8.2.1 信号输入/输出控制单元的数字逻辑电路晶体管和模拟电路电子元器件基础失效率评估和实施方法

评估和实施方法如下。

针对硬错误，基础失效率评估方法主要包含：

1) 使用业界公认的硬件元器件失效率数据，如根据 IEC/TR62380、IEC61709 或行业内等同标准中所描述的失效率计算公式推导得到；

注 1: 工业标准中所提供的失效率数据一般都比较保守。

2) 使用现场反馈或测试的统计数据；

3) 使用工程方法形成的专家判断，如现场经验、测试、可靠性分析等，具体方法如下。

注 2：针对数字逻辑与模拟电路失效率的计算应基于信号输入/输出控制单元的实际应用情况进行综合考虑，包含但不限于如下因素：物理电路类型、网表综合结果、芯片制程工艺、芯片使用工况等。

——通过加速寿命试验，可以有效地进行数字逻辑电路晶体管和模拟电路电子元器件基础失效率的测试。加速寿命试验的具体实施方法，具体可以参考国际国内相关标准。

——当实施加速寿命试验进行失效率测量时，为了使寿命测试中的温度修正到最大运行温度，需要启用加速因子。该计算使用了阿伦尼乌斯方程，其中涉及到的活化能值建议通过评估和验证方式获取。

——以样本中得到的故障数量作为输入，参与到$\chi 2$ 分布（卡方分布）函数计算中，并考虑所需的置信度水平，从而获得在整个测试群体中可能发生的总故障数量。

——针对软错误，基础失效率应依据国际国内相关标准中要求的测试方法来获得。

6.8.2.2 信号输入/输出控制单元数字逻辑电路和模拟电路失效模式及分布率评估和实施方法

评估和实施方法如下。

a）评估方法

评估方法如下：

1) 使用功能安全国际标准中的失效模式信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型电路失效模式；

注 1：功能安全标准中所列举的典型电路失效模式需根据芯片实际情况进行删减或补充

注 2：控制芯片信号输入/输出控制单元的典型失效模式示例参考附录 B。

2) 使用专家判断或根据芯片电路设计原理分析得到；

3) 使用验证工具进行故障注入或统计芯片测试过程中所观察到的失效模式，具体方法参照 b）实施方法中的步骤。

注 1：控制芯片信号输入/输出控制单元的故障注入示例参考附录 C。

注2：针对控制芯片信号输入/输出控制单元的故障注入应考虑IO/ADC等模拟电路与数字逻辑电路集成后的测试环境。

b）实施方法

在信号输入/输出控制单元的测试中，将测试功能电路的功能失效作为主要关注点，在被测试电路的特定位置注入所需的故障模型和失效模式，以表征被测试电路的功能失效。

测试实施的主要步骤包括（但不限于）：

1）选取故障点（实施故障注入的位置）及观测点（观察故障影响的位置）；

2）在选择的位置注入特定类型的故障，观测故障影响；

示例：如在 ADC 的逻辑控制电路注入故障，表征 ADC 的逻辑控制故障。

注：故障影响是指要素的失效对相关性的影响为安全故障，单点故障，或潜伏故障。

3）分析测试中获取的信息和数据，确定被测试项的定性结果（失效模式及影响）和定量结果（失效模式分布率）。

——在被测试项的定性结果方面，列出要素每种失效模式类型的影响。

——在被测试项的定量结果方面，统计要素故障注入后，被测试项失效模式的发生次数，计算各类型失效模式发生的比例。

注：失效模式分布是指被测试项各失效模式发生的比例。

6.8.2.3 输入/输出控制单元安全机制有效性及诊断覆盖率评估和实施方法

评估和实施方法如下。

a）评估方法

评估方法如下：

1）使用功能安全国际标准中的诊断覆盖率信息，如参考 GB/T34590.5 或 GB/T34590.11 中所列举的典型安全机制诊断覆盖率；

2）使用专家经验或根据安全机制设计原理进行数学推导得到；

3）使用验证工具进行故障注入并根据测试结果计算得到，具体方法参照 b）实施方法中的步骤。

注：控制芯片信号输入/输出控制单元的故障注入示例参考附录 C。

b）实施方法

测试用例的实施，主要是针对数字逻辑电路和模拟电路安全机制的有效性，测试实施的主要步骤包括（但不限于）：

1）使能相关测试项的安全机制；

2）选取故障点（实施故障注入的位置）以及诊断点（观察安全机制反应的位置）；

3）在选择的位置注入特定类型的故障，观测安全机制的动作和性能参数；

注1：注入特定类型的故障主要是指被测试项的物理故障模型，如Stuck at 0/1,floating等。

注2：安全机制的动作是指探测故障和处理故障，其中处理故障包括发出告警信号，置位相关故障状态位等。

注3：安全机制的性能参数是指故障探测时间间隔，故障响应时间间隔，安全机制的诊断覆盖率等。

4）记录测试中获取的信息和数据，确定被测试项的定性结果（安全机制的有效性）和定量结果（安全机制的诊断覆盖率）。

——在被测试项的定性结果方面，注入故障后，观测在一段时间内，安全机制能否正确处理故障，如发出告警信号，置位相关故障状态位等。

——在被测试项的定量结果方面，统计要素故障注入后，获取安全机制的故障探测时间间隔；故障响应时间间隔；以及安全机制的诊断覆盖率。

附 录 A

（资料性）

控制芯片 ASIL 等级评估方法计算示例：“硬件架构度量”

A.1 故障分类和诊断覆盖率

A.1.1 本要求适用于等级为 ASIL（B）、C 和 D 的安全目标。应为相关项的硬件定义硬件架构度量，且仅针对明显的潜在违背安全目标的安全相关硬件要素。

注：如果 ASIL 等级在括号中给出，则对于该 ASIL 等级，相应的章条应被认为是推荐而非要求。

A.1.2 本要求适用于等级为 ASIL（B）、C 和 D 的安全目标。应按照图 B.1 中阐明的，将发生在安全相关硬件要素上的每个故障归类为：

a) 单点故障

b) 残余故障

c) 多点故障;

注：多点故障的分类需要区分“潜伏多点故障”、“可探测的多点故障”和“可感知的多点故障”。

d) 安全故障

图A.1以图形方式表现了相关项中与安全相关硬件要素的故障分类：

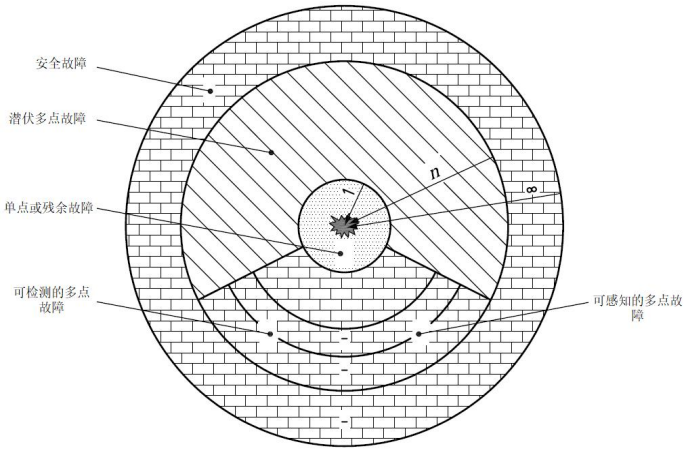

图 A.1 相关项中与安全相关的硬件要素的故障分类

在该图示中：

1 —— 距离 n 表示了在同一时刻存在的导致违背一个安全目标的独立故障的数量(n=1 对应单点故障或者残余故障，n=2 对应双点故障等)；

2 —— 距离等于 n 的故障位于圆环 n 和 n-1 之间的区域；除非在技术安全概念中表明相关，否则认为距离高于 n=2 的多点故障是安全故障。

因此每个安全相关硬件要素的失效率λ，都能按照等式(A.1)来表述（假设所有的失效都是互相独立的，且遵循指数分布），如下：

$$\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_{S} \quad \text{.....（A.1）}$$

式中：

λ_{SPF} —— 与硬件要素单点故障相关联的失效率；

λ_{RF} —— 与硬件要素残余故障相关联的失效率；

λ_{MPF} —— 与硬件要素多点故障相关联的失效率；

λ_{S} —— 与硬件要素安全故障相关联的失效率。

与硬件要素多点故障相关联的失效率，λ_{MPF}，能按照等式(A.2)来表述，如下：

$$\lambda_{\mathrm{MPF}} = \lambda_{\mathrm{MPF,DP}} + \lambda_{\mathrm{MPF,L}} \quad \text{.....（A.2）}$$

式中：

$\lambda_{MPF,\,DP}$ —— 与硬件要素可察觉或者可探测的多点故障相关联的失效率；

$\lambda_{MPF,\,L}$ —— 与硬件要素潜伏故障相关联的失效率。

分配给残余故障的失效率能用避免硬件要素的单点故障的安全机制的诊断覆盖率来确定。等式(A.3)提供了一个关于残余故障的失效率的保守估算。

$$\lambda_{RF} \le \lambda_{RF,\mathrm{est}} = \lambda \times \left(1 - \frac{K_{DC,RF}}{100\%}\right) \text{.....(A.3)}$$

式中：

$\lambda_{RF,\,est}$ —— 关于残余故障的估算的失效率；

$K_{DC,RF}$（也称为DC_{RF}）—— 关于残余故障的诊断覆盖率，用百分比表示。

分配给潜伏故障的失效率能用避免硬件要素的潜伏故障的安全机制的诊断覆盖率来确定。等式（A.4）提供了关于潜伏故障的失效率的保守估算：

$$\lambda_{MPF,\,L} \le \lambda_{MPF,\,L,\,\mathrm{est}} = \lambda \times \left(1 - \frac{K_{DC,\,MPF,\,L}}{100\%}\right) \text{.....（A.4）}$$

式中：

$\lambda_{MPF,L,\,est}$ —— 关于潜伏故障的估算的失效率；

$K_{DC,MPF,L}$（也称为$DC_{MPF,L}$）—— 关于潜伏故障的诊断覆盖率，用百分比表示。

注：如果上述估算被考虑的过于保守，则对于硬件要素失效模式的详细分析能将各个失效模式关联到针对特定安全目标的失效类别（单点故障、残余故障、可探测或可感知的潜伏多点故障、或者是安全故障），并确定分摊到各失效模式的失效率。

A.2 单点故障度量

A.2.1 这个度量反映了相关项通过安全机制覆盖或通过设计手段（主要为安全故障）实现的对单点故障和残余故障的鲁棒性。高的单点故障度量值意味着相关项硬件的单点故障和残余故障所占的比例低。

A.2.2 本要求适用于等级为 ASIL (B)、C 和 D 的安全目标。等式(A.5)中的计算应用于确定单点故障度量：

$$1-\frac{\sum_{SR,\ HW}\left(\lambda_{SPF}+\lambda_{RF}\right)}{\sum_{SR,\ HW}\lambda}=\frac{\sum_{SR,\ HW}\left(\lambda_{MPF}+\lambda_{S}\right)}{\sum_{SR,\ HW}\lambda} \quad \text{（A.5）}$$

式中：

$\sum_{SR,\ HW}(\lambda_X)$ —— 在度量中考虑的相关项安全相关硬件要素的 λ_x 总和。

注：图 A.2 给出了单点故障度量的图示。

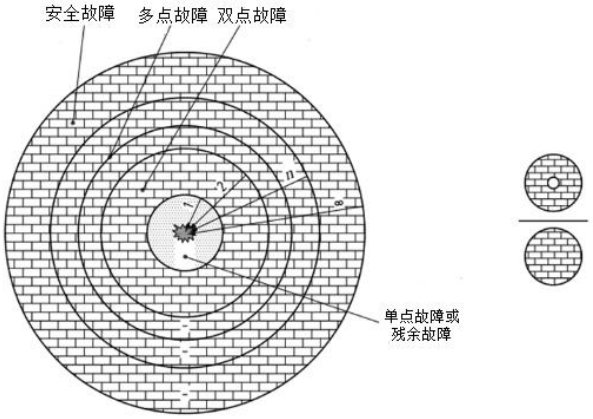

图 A.2 单点故障度量的图示

A.3 潜伏故障度量

A.3.1 这个度量反映了相关项通过安全机制覆盖、通过驾驶员在安全目标违背之前识别、或通过设计手段（主要为安全故障）实现的对潜伏故障的鲁棒性。高的潜伏故障度量值意味着硬件的潜伏故障所占的比例低。

A.3.2 本要求适用于等级为 ASIL(B)、(C)和 D 的安全目标。等式(A.6)中的计算应用于确定潜伏故障度量：

$$1-\frac{\sum_{\mathrm{SR,HW}}(\lambda_{\mathrm{MPF,L}})}{\sum_{\mathrm{SR,HW}}(\lambda-\lambda_{\mathrm{SPF}}-\lambda_{\mathrm{RF}})}=\frac{\sum_{\mathrm{SR,HW}}(\lambda_{\mathrm{MPF,DP}}+\lambda_{\mathrm{S}})}{\sum_{\mathrm{SR,HW}}(\lambda-\lambda_{\mathrm{SPF}}-\lambda_{\mathrm{RF}})} \quad \text{（A.6）}$$

式中：

$\sum_{\mathrm{SR,HW}}\lambda_x$ —— 在度量中考虑的相关项安全相关硬件要素的 λ_x 总和。

注：图 A.3 给出了潜伏故障度量的图示。

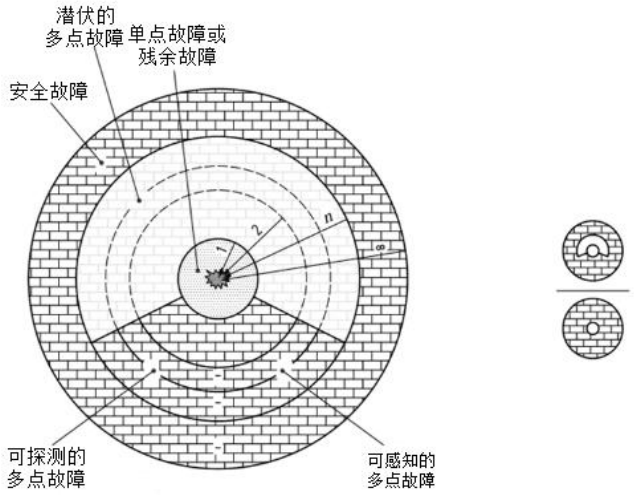

图 A.3 潜伏故障度量的图示

附 录 B

（资料性）

控制芯片典型失效模式示例

B.1 控制芯片内部电路示例

B.1.1 计算/逻辑控制单元主要元器件

与控制芯片计算/逻辑控制单元相关的主要元器件包括但不限于中央处理器，信号处理加速器，中断处理/路由单元等。

B.1.2 易失性/非易失性存储单元主要元器件

与控制芯片易失性/非易失性存储单元相关的主要元器件包括但不限于 ROM，eFLASH，eFLASH 控制单元，SRAM，SRAM 控制单元等。

B.1.3 片内/片外通信单元主要元器件

与控制芯片片内/片外通信单元相关的主要元器件包括但不限于内部总线互联，CAN 通信模块，SPI 通信模块，以太网通信模块等。

B.1.4 电源管理单元主要元器件

与控制芯片电源管理单元相关的主要元器件包括但不限于线性稳压器，开关型稳压器，电源控制单元等。

B.1.5 时钟管理单元主要元器件

与控制芯片时钟管理单元相关的主要元器件包括但不限于锁相环，时钟控制单元等。

B.1.6 信号输入/输出控制单元主要元器件

与控制芯片信号输入/输出控制单元相关的主要元器件包括但不限 ADC，DAC，IO 接口等。

B.2 控制芯片典型失效模式示例

结合 B.1 中所列计算/逻辑控制单元，易失性/非易失性存储单元，片内/片外通信单元，电源管理单元，时钟管理单元，以及信号输入/输出控制单元主要的元器件，控制芯片元器件典型失效模式示例如表 B.1 所示。

注：可以根据功能安全要求从表 B.1 所列典型失效模式中选取违背安全要求的元器件失效模式使用。

表 B.1 控制芯片元器件典型失效模式示例

控制器芯片电路组成	主要相关元器件	典型失效模式
计算/逻辑控制单元	中央处理器	CPU_FM1：给定指令流未执行（完全遗漏） CPU_FM2：非预期指令流被执行（误启动） CPU_FM3：指令流执行时间错误（过早/过晚） CPU_FM4：指令流结果不正确

表 B.1 控制芯片元器件典型失效模式示例（续）

控制器芯片电路组成	主要相关元器件	典型失效模式
计算/逻辑控制单元	信号处理加速器	SP_FM1：处理停滞，没有输出或输出定值（服务遗漏） SP_FM2：未请求的输出或中断（服务意外启动） SP_FM3：输出结构性损坏，例如，帧损坏（服务时间） SP_FM4：输出结构正常，但数据错误（服务值）
	中断处理/路由单元	ICU_FM1：对 CPU 的中断请求丢失 ICU_FM2：无触发事件时，向 CPU 请求中断 ICU_FM3：中断请求过早/过晚 ICU_FM4：中断请求发送错误数据
易失性/非易失性存储单元	ROM	ROM_FM1：卡滞 ROM_FM2：其他故障模型（例如卡滞开路故障、寻址故障、寻址延迟故障、转换故障、邻域模式敏感故障、感应晶体管缺陷、字线擦除干扰、位线擦除干扰、字线编程干扰、位线编程干扰等）
	eFLASH	eFLASH_FM1：卡滞 eFLASH_FM2：其他故障模型（例如卡滞开路故障、寻址故障、寻址延迟故障、转换故障、邻域模式敏感故障、感应晶体管缺陷、字线擦除干扰、位线擦除干扰、字线编程干扰、位线编程干扰等） eFLASH_FM3：软错误模型
	eFLASH控制单元	eFLASH_E_FM1：编程或擦除未被执行 eFLASH_E_FM2：未请求而被执行的编程或擦除操作 eFLASH_E_FM3：编程或擦除时间不正确 eFLASH_E_FM4：编程或擦除的内容错误 eFLASH_R_FM1：读取访问未被执行 eFLASH_R_FM2：未请求的读取访问 eFLASH_R_FM3：读取访问时间不正确 eFLASH_R_FM4：读取访问得到错误的内容
	SRAM	SRAM_FM1：卡滞 SRAM_FM2：其他故障模型（例如卡滞开路故障、寻址故障、寻址延迟故障、转换故障、邻域模式敏感故障等） SRAM_FM3：软错误模型
	SRAM控制单元	SRAM_RW_FM1：给定命令未执行（遗漏） SRAM_RW_FM2：非预期的命令被执行（误启动） SRAM_RW_FM3：命令结果延迟（过早/过晚） SRAM_RW_FM4：命令结果不正确 SRAM_HM_FM1：来自 SRAM 控制器的命令未执行（遗漏） SRAM_HW_FM2：非预期访问SRAM，例如。由瞬态故障引起的非预期访问 SRAM_HW_FM3：SRAM命令延迟（过早/过晚），例如，由内部时序生成导致的延迟

表 B.1 控制芯片元器件典型失效模式示例（续）

控制器芯片电路组成	主要相关元器件	典型失效模式
易失性/非易失性存储单元	SRAM 控制单元	SRAM_HW_FM4：最终 SRAM 数据损坏或写入到错误位置
片内/片外通信单元	内部总线互联	BUS_TXFR_FM1：请求的事务未送达 BUS_TXFR_FM2：无请求地发送事务 BUS_TXFR_FM3：在错误的时间发送事务 BUS_TXFR_FM4：以错误的数据发送事务
	CAN 通信模块 SPI 通信模块 以太网通信模块	COM_TX_FM1：请求的消息未被传输 COM_TX_FM2：未请求时，消息被传输 COM_TX_FM3：消息被传输过早/过晚 COM_TX_FM4：有错误值的消息被传输 COM_RX_FM1：传入消息未被处理 COM_RX_FM2：未请求时，消息被传输 COM_RX_FM3：消息被传输过早/过晚 COM_RX_FM4：有错误值的消息被传输
电源管理单元	线性稳压器 开关型稳压器	VR_FM1：输出电压高于规定范围的高阈值（即过压——OV） VR_FM2：输出电压低于规定范围的低阈值（即欠压——UV） VR_FM3：输出电压受尖峰影响 VR_FM4：启动时间不正确（即在预期范围之外） VR_FM5：输出电压精度太低，包括漂移 VR_FM6：输出电压在规定的范围内振荡
	线性稳压器 开关型稳压器	VR_FM7：输出电压受快速振荡影响，超出规定范围，但平均值在规定范围内 VR_FM8：静态电流（即保证稳压器内部电路正常工作需要的电流）超过最大值
	电源控制单元	VR_CON_FM1：给定的电源控制命令未执行（遗漏） VR_CON_FM2：非预期的电源控制命令被执行（误启动） VR_CON_FM3：电源控制命令结果延迟（过早/过晚） VR_CON_FM4：电源控制命令结果不正确
时钟管理单元	锁相环	PLL_FM1：输出卡滞（即高或低） PLL_FM2：输出浮空（即开路） PLL_FM3：不正确的输出信号频率（即超出预期范围，包括可用时的谐波，比如 EMC 辐射） PLL_FM4：不正确的输出信号的占空比（即超出预期范围） PLL_FM5：输出频率漂移 PLL_FM6：输出信号抖动过大 PLL_FM7：失锁状态（即相位误差，输出时钟与输入时钟不同步，但不会导致错误的频率和占空比） PLL_FM8：输出信号中缺少脉冲 PLL_FM9：输出信号中出现额外的脉冲
	时钟控制单元	CL_CON_FM1：给定的时钟控制命令未执行（遗漏） CL_CON_FM2：非预期的时钟控制命令被执行（误启动）

表 B.1 控制芯片元器件典型失效模式示例（续）

控制器芯片电路组成	主要相关元器件	典型失效模式
时钟管理单元	时钟控制单元	CL_CON_FM3：时钟控制命令结果延迟（过早/过晚） CL_CON_FM4：时钟控制命令结果不正确
信号输入/输出控制单元	ADC	ADC_FM1：一路或多路输出卡滞（即高或低） ADC_FM2：一路或多路输出浮空（即开路） ADC_FM3：精度误差（即误差超过LSB）
控制芯片电路组成	主要相关元器件	典型失效模式
信号输入/输出控制单元	ADC	ADC_FM4：偏移误差（不包括输出上的卡滞或浮空，低分辨率） ADC_FM5：无单调转换特性（即给定两个输入模拟电压V1>V2，相应的数字值为D1<D2） ADC_FM6：满量程误差（不包括输出上的卡滞或浮空，低分辨率） ADC_FM7：单调转换曲线的线性误差（不包括输出上的卡滞或浮空，低分辨率） ADC_FM8：不正确的建立时间（即超出预期范围）
	DAC	DAC_FM1：输出卡滞（即高或低） DAC_FM2：输出浮空（即开路） DAC_FM3：偏移误差（不包括输出上的卡滞或浮空，低分辨率） DAC_FM4：单调转换的线性误差（不包括输出上的卡滞或浮空，低分辨率） DAC_FM5：满量程增益误差（不包括输出上的卡滞或浮空，低分辨率） DAC_FM6：非单调转换 DAC_FM7：不正确的建立时间（即超出预期范围） DAC_FM8：输出信号的振荡，包括漂移
	IO接口	IO_FM1：输出卡滞（即高或低） IO_FM2：输出浮空（即开路）

附 录 C

（资料性）

控制芯片 ASIL 等级评估方法测试示例：“故障注入测试”

C.1 故障注入方法描述

故障注入方法是芯片功能安全验证与测试领域的重要技术手段。本文件中所阐述的测试方法，采用故障注入技术对控制芯片的安全架构及安全机制进行验证与测试，旨在评估相关的失效模式及失效模式占比，安全机制的有效性及诊断覆盖率，从而确认该类芯片的 ASIL。

C.2 故障注入方法示例

C.2.1 针对计算/逻辑控制单元的故障注入

针对计算/逻辑控制单元的故障注入，可以通过 EDA 工具，FPGA 测试及硅后测试来实施故障注入，从而评估相关失效模式及失效模式占比，安全机制有效性及诊断覆盖率。例如，针对中央处理器的双核锁步安全机制：

a） 在 EDA 工具仿真中，首先准备好中央处理器验证环境，而后针对双核锁步看护的电路设计对应的测试用例，主要对比主 CPU 输出与冗余 CPU 输出，通过运行 EDA 工具对电路进行分析，根据生成的故障点，类型及安全机制响应可以得到失效模式，失效模式占比及安全机制有效性，而后经过计算即可得出双核锁步安全机制针对中央处理器失效的诊断覆盖率；

b） 在 FPGA 测试中，首先搭建好 FPGA 测试环境，配置使能寄存器使能中央处理器的双核锁步安全机制，而后通过配置故障注入使能寄存器进行故障注入，最后检查报警处理模块双核锁步安全机制对应的报警信号及报警状态是否有效，来检查安全机制的有效性；

c） 在硅后测试中，首先搭建好搭载了控制芯片评估板的测试环境，而后配置使能寄存器与故障注入寄存器进行中央处理器的双核锁步安全机制故障注入，最后检查报警处理模块双核锁步安全机制对应的报警信号及报警状态是否有效，来检查安全机制的有效性。

C.2.2 针对易失性/非易失性存储单元的故障注入

针对易失性/非易失性存储单元的故障注入，可以通过 EDA 工具，FPGA 测试及硅后测试来实施故障注入，从而评估相关失效模式及失效模式占比，安全机制有效性及诊断覆盖率。例如，针对 SRAM 的 ECC 机制：

a） 在 EDA 工具仿真中，首先准备好 SRAM 验证环境，而后针对 ECC 机制看护的内存设计对应的测试用例，主要检查其在 SRAM 不同 bit 数量及失效位置的情况下 ECC 能否正确的处理故障，通过运行 EDA 工具对电路进行分析，根据生成的故障点，类型及安全机制响应可以得到失效模式，失效模式占比及安全机制有效性，而后经过计算即可得出 ECC 针对 SRAM 存储错误失效的诊断覆盖率；

b） 在 FPGA 测试中，首先搭建好 FPGA 测试环境，配置使能寄存器使能 SRAM 的 ECC 机制，而后通过故障注入配置寄存器，选择注入故障的 bit 个数及位置，最后检查是否正确的检测出与注入 bit 个数及位置相符合的故障并生成了对应的报警信号及报警状态，来检查安全机制的有效性；

c） 在硅后测试中，首先搭建好搭载了控制芯片评估板的测试环境，配置安全机制使能寄存器及 ECC 故障注入配置寄存器，选择注入故障的 bit 个数及位置，最后检查是否正确的检测出与注入 bit 个数及位置相符合的故障并生成了对应的报警信号及报警状态，来检查安全机制的有效性。

C.2.3 针对片内/片外通信单元的故障注入

针对片内/片外通信单元的故障注入，可以通过 EDA 工具，FPGA 测试及硅后测试来实施故障注入，从而评估相关失效模式及失效模式占比，安全机制有效性及诊断覆盖率。例如，针对内部总线互联的信号 Parity 校验机制：

a） 在 EDA 工具仿真中，首先准备好内部总线互联验证环境，而后针对信号 Parity 校验看护的电路设计对应的测试用例，主要检查其在总线信号不同 bit 数量失效的情况下 Parity 能否正确的检测故障，通过运行 EDA 工具对电路进行分析，根据生成的故障点，类型及安全机制响应可以得到失效模式，失效模式占比及安全机制有效性，而后经过计算即可得出 Parity 校验机制针对内部总线互联的信号失效的诊断覆盖率；

b） 在 FPGA 测试中，首先搭建好 FPGA 测试环境，配置使能寄存器使能总线的安全机制，而后通过配置故障注入使能寄存器注入 Parity 错误，最后检查报警处理模块总线 Parity 校验安全机制对应的报警信号及报警状态是否有效，来检查安全机制的有效性；

c） 在硅后测试中，首先搭建好搭载了控制芯片评估板的测试环境，而后配置使能寄存器与故障注入寄存器进行总线信号的 Parity 校验安全机制故障注入，最后检查报警处理模块总线 Parity 校验安全机制对应的报警信号及报警状态是否有效，来检查安全机制的有效性。

C.2.4 针对电源管理单元的故障注入

针对电源管理单元的故障注入，可以通过 EDA 工具，FPGA 测试及硅后测试来实施故障注入，从而评估相关失效模式及失效模式占比，安全机制有效性及诊断覆盖率。但针对电源管理单元部分模拟电路相关的安全机制，FPGA 存在一定局限性，一般通过 EDA 工具与硅后测试进行相应的验证。例如，针对线性稳压器的过压/欠压检测机制：

a） 在 EDA 工具仿真中，首先准备好电源管理单元验证环境，而后针对过压/欠压检测机制看护的线性稳压器数字电路设计对应的测试用例，主要检查其在线性稳压器数字电路部分不同门级电路失效的情况下过压/欠压能否检测对应的失效，通过运行 EDA 工具对电路进行分析，根据生成的故障点，类型及安全机制响应可以得到失效模式，失效模式占比及安全机制有效性，而后经过计算即可得出过压/欠压检测机制针对线性稳压器数字电路部分失效的诊断覆盖率；

b） 在硅后测试中，首先搭建好搭载了控制芯片评估板的测试环境，而后通过配置过压及欠压的监控阈值以及使用可编程电源等设备根据特定步长逐步调整电压，来模拟注入过压及欠压故障，经过过压/欠压检测的抖动时间后，检查报警处理模块线性稳压器过压/欠压检测机制对应的报警信号及报警状态是否有效，来检查安全机制的有效性。

C.2.5 针对时钟管理单元的故障注入

针对时钟管理单元的故障注入，可以通过 EDA 工具，FPGA 测试及硅后测试来实施故障注入，从而评估相关失效模式及失效模式占比，安全机制有效性及诊断覆盖率。例如，针对时钟控制单元的锁相环频率监控机制：

a） 在 EDA 工具仿真中，首先准备好时钟管理单元验证环境，而后针对频率监控看护的电路设计对应的测试用例，主要检查其在锁相环电路失效的情况下频率监控机制能否正确的检测故障，通过运行 EDA 工具对电路进行分析，根据生成的故障点，类型及安全机制响应可以得到失效模式，失效模式占比及安全机制有效性，而后经过计算即可得出频率监控机制对锁相环失效的诊断覆盖率；

b） 在 FPGA 测试中，首先搭建好 FPGA 测试环境，使用多个时钟源例如额外的信号发生器，而后通过改变频率监控机制的参考时钟来模拟注入锁相环频率超限的故障，最后检查报警处理模块时钟控制单元锁相环频率监控机制对应的报警信号及报警状态是否有效，来检查安全机制的有效性；

c） 在硅后测试中，首先搭建好搭载了控制芯片评估板的测试环境，而后通过配置锁相环频率监控机制的阈值来模拟锁相环频率超限的故障，最后检查报警处理模块时钟控制单元锁相环频率监控机制对应的报警信号及报警状态是否有效，来检查安全机制的有效性。

C.2.6 针对信号输入/输出控制单元的故障注入

针对信号输入/输出控制单元的故障注入，可以通过 EDA 工具，FPGA 测试及硅后测试来实施故障注入，从而评估相关失效模式及失效模式占比，安全机制有效性及诊断覆盖率。但针对信号输入/输出控制单元部分模拟电路相关的安全机制，FPGA 存在一定局限性，一般通过 EDA 工具与硅后测试进行相应的验证。例如，针对 ADC 的开路检测机制：

a） 在 EDA 工具仿真中，首先准备好信号输入/输出控制单元验证环境，而后针对 ADC 开路检测机制看护的电路设计对应的测试用例，主要检查其在 ADC 数字电路部分不同门级电路失效的情况下 ADC 开路检测机制能否检测出对应的失效，通过运行 EDA 工具对电路进行分析，根据生成的故障点，类型及安全机制响应可以得到失效模式，失效模式占比及安全机制有效性，而后经过计算即可得出 ADC 开路检测机制针对 ADC 数字电路部分失效的诊断覆盖率；

b） 在硅后测试中，首先搭建好搭载了控制芯片评估板的测试环境，完成配置 ADC 开路检测安全机制并使用不同的方式断开 ADC 对应通道的外部负载，如使用开关矩阵断开负载，重复多次；串联可变电阻，通过不同的阻值检测开路检测机制能否在预设的阻值阈值预期检测出故障等。最后检查报警处理模块 ADC 开路检测安全机制对应的报警信号及报警状态是否有效，来检查安全机制的有效性。

参考文献

[1] GB T 34590.5-2022 道路车辆 功能安全 第5部分：产品开发：硬件层面
[2] GB T 34590.8-2022 道路车辆 功能安全 第8部分：支持过程
[3] GB T 34590.11-2022 道路车辆 功能安全 第11部分：半导体应用指南