ICS 43.040

CCS T 35

中华人民共和国国家标准

GB/T 34590.5—XXXX

代替 GB/T 34590.5-2017

道路车辆 功能安全

第5部分：产品开发：硬件层面

Road vehicles-Functional safety-

Part 5:Product development at the hardware level

(ISO 26262-5:2018,MOD)

（征求意见稿）

（本草案完成时间：2021年4月1日））

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

GB/T 34590-XXXX《道路车辆 功能安全》分为以下部分：

——第 1 部分：术语；

——第 2 部分：功能安全管理；

——第 3 部分：概念阶段；

——第 4 部分：产品开发：系统层面；

——第 5 部分：产品开发：硬件层面；

——第 6 部分：产品开发：软件层面；

——第 7 部分：生产、运行、服务和报废；

——第 8 部分：支持过程；

——第 9 部分：以汽车安全完整性等级为导向和以安全为导向的分析；

——第 10 部分：指南；

——第 11 部分：半导体应用指南；

——第 12 部分：摩托车的适用性。

本文件为GB/T 34590-XXXX的第5部分。

本文件代替GB/T 34590.5-2017《道路车辆 功能安全 第5部分：产品开发：硬件层面》，与GB/T 34590.5-2017相比，主要变化如下：

——修改了标准适用范围，由“量产乘用车”扩大到“除轻便摩托车外的量产道路车辆”；

——新增了对商用车辆的相关要求和示例、对摩托车的适应性要求等；

——增加了硬件规范（来自外部）(见 6.3.2)；

——增加了注 2（见 6.4.2）；

——增加了注释（见 6.4.7）；

——增加了关于目的的内容（见 7.1）；

——增加了非安全相关的硬件需求规范（来自外部）(见 7.3.2)；

——增加了注 1、注 2，表 1 由“模块化的硬件设计原则”更改为“硬件架构设计原则”(见 7.4.1.6)；

——增加了对噪声因素的要求(见 7.4.1.7)；

——增加了注 6 以及对 ASIL（A）的要求(见 7.4.3.3)；

——增加了对 ASIL（A）的要求(见 7.4.3.4)；

——增加了注 5、注 6(见 7.4.3.5)；

——增加了硬件设计验证方法提供证据证明的要求(见 7.4.4.1)；

——增加了验证 SEooC 的假设的有效性的要求(见 7.4.4.3)；

——增加了硬件设计过程中产生的硬件要素的生产、运行、服务和报废要求(见 7.4.5.5)；

——增加了注 2（见 8.2）；

——增加了注 2、注 3、注 4、注 5、注 7、注 8、注 9、注 10、示例 2、示例 3（见 8.4.3）；

——增加了注 2 以及列项 a、b 中关于“附加的安全机制”的要求（见 8.4.4）；

——增加了关于 SPFM 目标值相关公式的示例（见 8.4.7）；

——增加了示例 1、示例 2 中关于“附录 H 提供的示例”以及“LFM 目标值相关公式”的内容（见 8.4.8）；

——增加了关于“本要求的 ASIL 适用等级”的内容（见 9.4.1.1）；

——增加了“证明单一硬件元器件单点故障发生概率足够低”的论据的内容（见 9.4.1.2）；

——增加了“证明一个硬件元器件的残余故障发生概率足够低”的论据的内容（见 9.4.1.3）；

——增加了注 1、注 2（见 9.4.2.1）；

——增加了注 3、注 4、注 5（见 9.4.2.2）；

——增加了构成相关项的多个系统的要求（见 9.4.2.3）；

——增加了注 8（见 9.4.2.4）；

——增加了注 3、注 4（见 9.4.3.2）；

——增加了适用的 ASIL 等级（见 9.4.3.4）；

——增加了示例和注 5（见 9.4.3.11）；

——增加了双点失效可接受的条件的要求（见 9.4.3.12）；

——增加了关于“在不能满足 9.4.3.11 或 9.4.3.12 的要求的情况下导致可能的双点失效的条件”的内容（见 9.4.3.13）；

——增加了示例以及对安全相关硬件元器件的要求（见 10.4.3）；

——增加了硬件集成和验证规范（见 10.5.1）；

——增加了部分公式，且对原有公式进行了删减修订（见 C.1.2）；

——增加了可集成在组件中的安全机制的注释（见附录 D）；

——增加了示例（见 D.2.2.2）；

——增加了附录 F、附录 G、附录 H。

——删除了 5.3、5.4、5.5 中关于“本章输入、要求和建议、工作成果”的内容；

——删除了“安全计划（细化的）”（见 6.3.1）；

——删除了注 1（见 6.4.2）；

——删除了注释（见 6.4.3）；

——删除了关于目的的内容（见 2017 版的 7.1）；

——删除了安全计划（细化的）（见 7.3.1）；

——删除了注（见 9.2）；

——删除了关于“比例因子”的内容（见 9.4.2.7）；

——删除了 2017 版的注 3（见 9.4.3.2）；

——删除了失效率换算的内容（见 2017 版的 9.4.3.12）；

——删除了硬件安全需求规范、硬件设计规范（见 10.3.1）；

——删除了项目计划（细化的）（见 10.3.2）；

——删除了 2017 版的表 D.5、D.6、D.13、D.14；

——删除了 2017 版的 D.2.4、D.2.5；

——删除了 2017 版的附录 E 注 4。

——修改了第 5 章的标题；

——修改了关于目的的描述（见 5.1）；

——修改了图 2（见 5.2）；

——修改了总则的描述（见 9.2）；

——修改了第 10 章的标题；

——修改了表 12 的标题（见 10.4.6）；

——修改了表 D.1 的标题、注释；

——修改了 D.2.2.2 的标题；

——图 E.2 修改为表 E.1；

——修改了表 E.1 的注 5 重的计算数据；

——图 E.3 修改为表 E.2；

本文件使用重新起草法修改采用了ISO 26262-5：XXXX 《道路车辆 功能安全 第5部分：产品开发：硬件层面》。

本文件与ISO 26262-5：2018的技术性差异及其原因如下：

——关于规范性引用文件，本文件做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第 2 章“规范性引用文件”中，具体调整如下：

用修改采用国际标准的GB/T 34590.1-XXXX代替ISO 26262-1：2018；

用修改采用国际标准的GB/T 34590.2-XXXX代替ISO 26262-2：2018；

用修改采用国际标准的GB/T 34590.4-XXXX代替ISO 26262-4：2018；

用修改采用国际标准的GB/T 34590.6-XXXX代替ISO 26262-6：2018；

用修改采用国际标准的GB/T 34590.7-XXXX代替ISO 26262-7：2018；

用修改采用国际标准的GB/T 34590.8-XXXX代替ISO 26262-8：2018；

用修改采用国际标准的GB/T 34590.9-XXXX代替ISO 26262-9：2018。

本文件做了下列编辑性修改：

——将国际标准中的“本国际标准”改为“本文件”；

——删除国际标准的前言；

——修改国际标准的引言及其表述。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会（SAC/TC114）归口。

本文件起草单位：

本文件主要起草人：

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会（SAC/TC114）归口。

本文件起草单位：

本文件主要起草人：

本文件所代替文件的历次版本发布情况为：

——GB/T 34590.5,2017 年首次发布。

引　言

ISO 26262是以IEC 61508为基础，为满足道路车辆上电气/电子系统的特定需求而编写。

GB/T 34590修改采用ISO 26262，适用于道路车辆上由电子、电气和软件组件组成的安全相关系统在安全生命周期内的所有活动。

安全是道路车辆开发的关键问题之一。汽车功能的开发和集成强化了对功能安全的需求，以及对提供证据证明满足功能安全目标的需求。

随着技术日益复杂、软件和机电一体化应用不断增加，来自系统性失效和随机硬件失效的风险逐渐增加，这些都在功能安全的考虑范畴之内。GB/T 34590通过提供适当的要求和流程来降低风险。

为了实现功能安全，GB/T 34590-XXXX（所有部分）：

a) 提供了一个汽车安全生命周期（开发、生产、运行、服务、报废）的参考，并支持在这些生命周期阶段内对执行的活动进行剪裁；

b) 提供了一种汽车特定的基于风险的分析方法，以确定汽车安全完整性等级（ASIL）；

c) 使用 ASIL 等级来定义 GB/T 34590 中适用的要求，以避免不合理的残余风险；

d) 提出了对于功能安全管理、设计、实现、验证、确认和认可措施的要求；及

e) 提出了客户与供应商之间关系的要求。

GB/T 34590针对的是电气/电子系统的功能安全,通过安全措施(包括安全机制)来实现。它也提供了一个框架，在该框架内可考虑基于其它技术（例如，机械、液压、气压）的安全相关系统。

功能安全的实现受开发过程（例如，包括需求规范、设计、实现、集成、验证、确认和配置）、生产过程、服务过程和管理过程的影响。

安全问题与常规的以功能为导向和以质量为导向的活动及工作成果相互关联。GB/T 34590 涉及与安全相关的开发活动和工作成果。

图 1 为 GB/T 34590 的整体架构。GB/T 34590 基于 V 模型为产品开发的不同阶段提供参考过程模型：

——阴影”V”表示 GB/T 34590.3-XXXX、GB/T 34590.4-XXXX、GB/T 34590.5-XXXX、GB/T 34590.6-XXXX、GB/T 34590.7-XXXX 之间的相互关系；

——对于摩托车：

GB/T 34590.12-XXXX的第8章支持GB/T 34590.3-XXXX；

GB/T 34590.12-XXXX的第9章和第10章支持GB/T 34590.4-XXXX。

——以“m-n”方式表示的具体章条中，“m”代表特定部分的编号，“n”代表该部分章的编号。

示例：“2-6”代表GB/T 34590.2-XXXX的第6章。

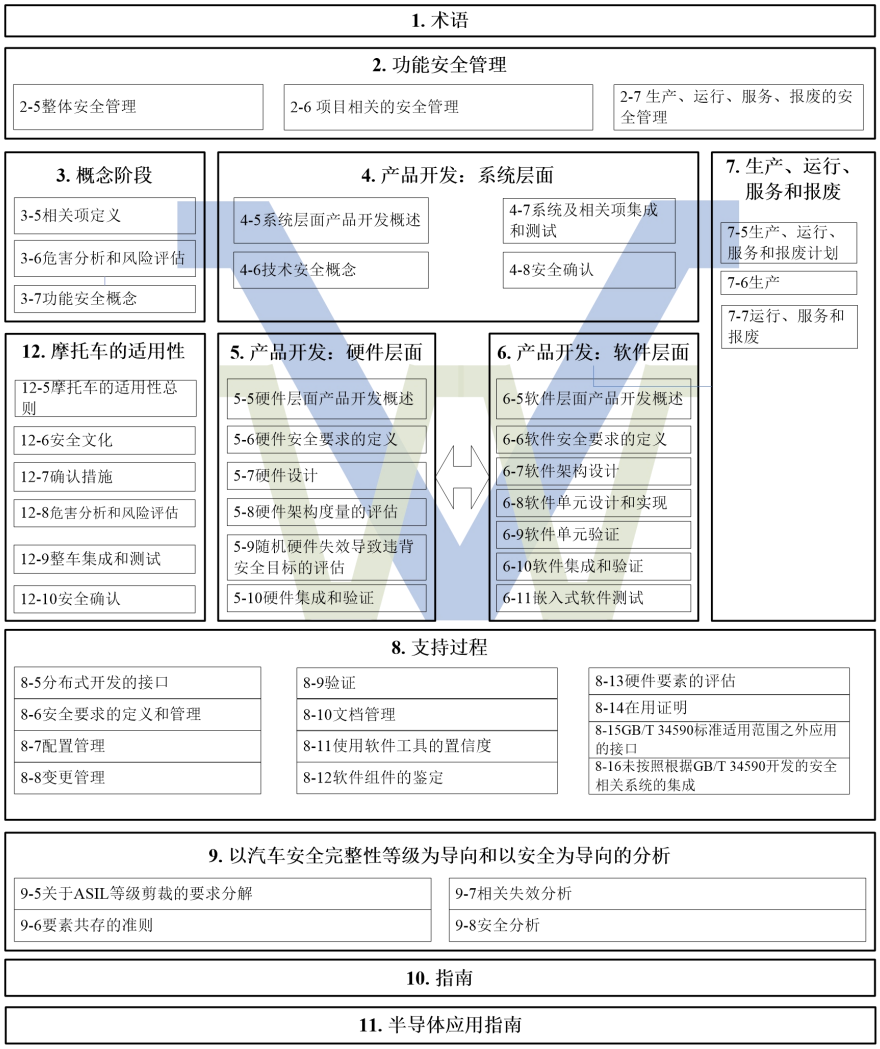


图 1　GB/T 34590-XXXX 概览

道路车辆 功能安全
第5部分：产品开发：硬件阶段

1 范围

GB/T 34590的本部分规定了车辆在硬件层面产品开发的要求，包括：

——硬件层面产品开发的概述；

——硬件安全要求的定义；

——硬件设计；

——硬件架构度量的评估；

——因随机硬件故障而导致违背安全目标的评估；及

——硬件集成和验证。

本文件适用于安装在除轻便摩托车外的量产道路车辆上的包含一个或多个电气/电子系统的与安全相关的系统。

本文件不适用于特殊用途车辆上特定的电气/电子系统，例如，为残疾驾驶者设计的车辆。

注：其他专用的安全标准可作为本文件的补充，反之亦然。

已经完成生产发布的系统及其组件或在本文件发布日期前正在开发的系统及其组件不适用于本文件。对于在本文件发布前完成生产发布的系统及其组件进行变更时，本文件基于这些变更对安全生命周期的活动进行裁剪。未按照本文件开发的系统与按照本文件开发的系统进行集成时，需要按照本文件进行安全生命周期的裁剪。

本文件针对由安全相关的电气/电子系统的功能异常表现而引起的可能的危害，包括这些系统相互作用而引起的可能的危害。本文件不针对与触电、火灾、烟雾、热、辐射、毒性、易燃性、反应性、腐蚀性、能量释放等相关的危害和类似的危害，除非危害是直接由安全相关的电气/电子系统的功能异常表现表现而引起的。

本文件提出了安全相关的电气/电子系统进行功能安全开发的框架，该框架旨在将功能安全活动整合到企业特定的开发框架中。本文件规定了为实现产品功能安全的技术开发要求，也规定了组织应具备相应功能安全能力的开发流程要求。

本文件不针对电气/电子系统的标称性能。

本文件中对硬件要素的要求适用于非可编程和可编程硬件要素，如ASIC、FPGA和PLD，更多指南见GB/T 34590.10-XXXX和GB/T 34590.11-XXXX。

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 34590.1-XXXX 道路车辆 功能安全 第1部分：术语(ISO 26262-1:2018,MOD)

GB/T 34590.2-XXXX 道路车辆 功能安全 第2部分：功能安全管理(ISO 26262-2:2018,MOD)

GB/T 34590.4-XXXX 道路车辆 功能安全 第4部分：产品开发：系统层面(ISO 26262-4:2018,MOD)

GB/T 34590.6-XXXX 道路车辆 功能安全 第6部分：产品开发：软件层面(ISO 26262-6:2018,MOD)

GB/T 34590.7-XXXX 道路车辆 功能安全 第7部分：生产、运行、服务和报废(ISO 26262-7:2018,MOD)

GB/T 34590.8-XXXX 道路车辆 功能安全 第8部分：支持过程(ISO 26262-8:2018,MOD)

GB/T 34590.9-XXXX，道路车辆 功能安全 第9部分：以汽车安全完整性等级为导向和以安全为导向的分析(ISO 26262-9:2018，MOD)

3 术语、定义和缩略语

GB/T 34590.1-XXXX界定的术语、定义和缩略语适用于本文件。

4 要求

4.1 目的

本章规定了：

a) 如何符合 GB/T 34590-XXXX；

b) 如何解释 GB/T 34590-XXXX 中所使用的表格；及

c) 如何解释各章条基于不同的 ASIL 等级的适用性。

4.2 一般要求

如声明满足GB/T 34590-XXXX的要求时，应满足每一个要求，除非有下列情况之一：

a) 按照 GB/T XXXXX.2-XXXX 的要求，安全活动的剪裁已经实施并表明这些要求不适用；或

b) 不满足要求的理由存在且是可接受的，并且按照 GB/T XXXXX.2-XXXX 的要求对该理由进行了评估。

标有“注”或“示例”的信息仅用于辅助理解或阐明相关要求，不应作为要求本身且不具备完备性。

将安全活动的结果作为工作成果。应具备上一阶段工作成果作为“前提条件”的信息。如果章条的某些要求是依照ASIL定义的或可剪裁的，某些工作成果可不作为前提条件。

“支持信息”是可供参考的信息，但在某些情况下，GB/T 34590-XXXX不要求其作为上一阶段的工作成果，并且可以是由不同于负责功能安全活动的人员或组织等外部资源提供的信息。

4.3 表的诠释

本文件中的表是规范性或资料性取决于上下文。在满足相关要求时，表中列出的不同方法有助于置信度水平。表中的每个方法是：

a) 一个连续的条目（在最左侧列以顺序号标明，如 1、2、3）；或

b) 一个选择的条目（在最左侧列以数字后加字母标明，如 2a、2b、2c）。

对于连续的条目，高度推荐和推荐的方法按照ASIL等级推荐予以使用。高度推荐或推荐的方法允许用未列入表中的其它方法替代,此种情况下，应给出满足相关要求的理由。如果可以给出不选择所有条目也能符合相应要求的理由，则不需要对缺省方法做进一步解释。

对于选择性的条目，应按照指定的ASIL等级对这些方法进行适当的组合，而与这些方法在表中是否列出无关。如果所列出的方法对于一个ASIL等级来说具有不同的推荐等级，宜采用具有较高推荐等级的方法。应给出选择组合方法或选择单一方法满足相应要求的理由。

注：在表中所列出方法的理由是充分的。但是，这并不意味着有倾向性或对未列到表中的方法表示反对。

对于每种方法，应用相关方法的推荐等级取决于ASIL等级，分类如下：

——“++”表示对于指定的 ASIL 等级，高度推荐该方法；

——“+” 表示对于指定的 ASIL 等级，推荐该方法；

——“o” 表示对于指定的 ASIL 等级，不推荐也不反对该方法。

4.4 基于 ASIL 等级的要求和建议

若无其它说明，对于ASIL A、 B、 C和D等级，应满足每一章条的要求或建议。这些要求和建议参照安全目标的ASIL等级。如果在项目开发的早期对ASIL等级完成了分解，按照GB/T XXXXX-9第5章的要求，应遵循分解后的ASIL等级。

如果GB/T 34590-XXXX中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。这里的括号与ASIL等级分解无关。

4.5 摩托车的适用性

对于适用于GB/T XXXXX.12要求的摩托车的相关项或要素，GB/T 34590.12的要求替代本部分和GB/T 34590.2的相应要求。

4.6 卡车、客车、挂车和半挂车的适用性

对卡车、客车、挂车和半挂车的特殊规定以（T&B）来表示。

5 硬件层面产品开发的概述

5.1 目的

本章的目的是描述硬件开发各子阶段中的功能安全活动。

5.2 总则

按照GB/T 34590.2-XXXX,6.4.6来制定满足安全要求的硬件开发所需的活动和流程的计划。

图2阐明了为满足本文件要求的硬件层面产品开发的流程步骤，以及在GB/T 34590框架内这些步骤的集成。

硬件层面产品开发的必要活动和流程包括：

——技术安全概念的硬件实现；

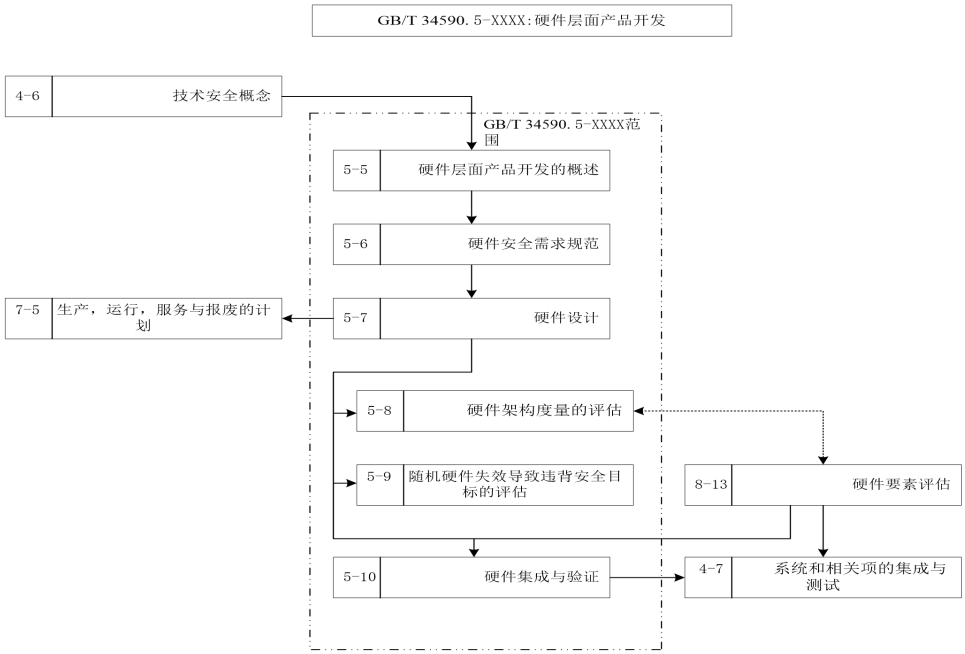
——分析潜在的硬件故障及其影响；及

——与软件开发的协调。

与软件开发子阶段相比，本文件包含两个章节，描述了对相关项整体硬件架构的定量评估。

第8章描述了两个度量，以评估相关项硬件架构和实施的安全机制应对随机硬件失效的有效性。

作为对第8章的补充，第9章描述了两种可选的方法以评估违背安全目标的残余风险是否足够低，一种是应用全局概率方法（请参阅9.4.2，PMHF方法），另一种是应用割集分析方法（请参阅EEC方法9.4.3），来研究硬件要素中所识别出每个故障对违背安全目标的影响。



注：在图中，GB/T 34590的每个部分的具体章用以下方式表示：“ m-n”，其中“ m”代表部分的编号，“ n”代表章的编号，例如 “ 4-7”代表GB/T 34590.4-XXXX第4部分第7章。

图 2 硬件层面产品开发参考阶段模型

6 硬件安全要求的定义

6.1 目的

本章的目的是：

a) 定义硬件安全要求。这些要求由技术安全概念和系统架构设计规范导出；

b) 细化最初在 GB/T 34590.4-XXXX，6.4.7 中定义的软硬件接口规范；及

c) 验证硬件安全要求及软硬件接口规范与技术安全概念及系统架构设计规范的一致性。

6.2 总则

将技术安全要求分配给硬件和软件。既分配给硬件又分配给软件的要求被进一步划分出仅对硬件的安全要求。考虑设计限制和这些限制对硬件的影响，对硬件安全要求进行进一步的细化。

6.3 本章的输入

6.3.1 前提条件

应具备如下信息：

——技术安全概念，按照 GB/T 34590.4-XXXX，6.5.2；

——系统架构设计规范，按照 GB/T 34590.4-XXXX，6.5.3；及

——软硬件接口规范，按照 GB/T 34590.4-XXXX，6.5.4。

6.3.2 支持信息

可以考虑如下信息：

——软件安全需求规范（请参见 GB/T 34590.6-XXXX，6.5.1）；及

——硬件规范（来自外部）。

6.4 要求和建议

6.4.1 相关项硬件要素的硬件安全需求规范应从分配给硬件的技术安全要求中导出（源自 GB/T 34590.4-XXXX，6.5.2）。

6.4.2 硬件安全需求规范应包括与功能安全有关的每一条硬件要求，包括以下内容：

a) 为控制要素硬件内部失效的硬件安全要求和安全机制的相关特性。这包括用于覆盖瞬态故障(例如，由于所使用的技术而产生的瞬态故障)的内部安全机制；

示例 1：特性可能包括看门狗的定时和探测能力。

b) 为控制或者容忍要素外部失效的硬件安全要求和安全机制的相关特性；

示例 2：当外部失效发生时，如 ECU 的输入开路时，要求 ECU 应具备的功能表现。

c) 为符合其他要素的安全要求的硬件安全要求和安全机制的相关特性；

示例 3：对传感器或执行器的诊断。

d) 为探测内外部失效和发送失效信息的硬件安全要求和安全机制的相关特性；及

注 1：d）中描述的硬件安全要求包括防止故障潜伏的安全机制。

示例 4：安全机制中定义的硬件元器件的故障响应时间，要符合故障容错时间间隔。

e) 不定义安全机制的硬件安全要求。

示例 5：举例如下：

——为满足 6.4.3 和 6.4.4 所描述的随机硬件失效目标值的硬件要素要求；

——为避免特定行为的要求（例如，“一个特定的传感器不应该有一个不稳定的输出”）；

——分配给执行预期功能的硬件要素的要求；及

——定义线束或接插件的设计措施的要求。

注 2：安全机制能用硬件、软件或软硬件结合的方式来实现。

6.4.3 本要求适用于等级为 ASIL（B），C 和 D 的安全目标。当为相关项硬件要素推导目标值时，应考虑按照 GB/T 34590.4-XXXX，6.4.5 的要求，为本文件第 8 章定义的度量设定目标值。

6.4.4 本要求适用于等级为 ASIL（B），C 和 D 的安全目标。当为相关项硬件要素推导目标值时，应考虑按照 GB/T 34590.4-XXXX，6.4.5 的要求，为本文件第 9 章定义的过程设定目标值。

注：除非同意使用9.4.3的EEC，否则在GB/T 34590.8-XXXX 第5章定义的分布式开发情况下，此活动可能包括PMHF目标值的分配。

6.4.5 硬件安全要求应按照 GB/T 34590.8-XXXX 第 6 章的要求进行定义。

6.4.6 应定义相关项的硬件要素的设计验证准则，包括环境条件（温度、振动、EMI 等）、特定的运行环境（供电电压、任务剖面等）以及组件的特定要求：

a) 通过硬件要素评估进行的验证，其准则应满足 GB/T 34590.8-XXXX 第 13 章的要求；及

b) 通过测试进行的验证，其准则应满足本文件第 10 章的要求。

6.4.7 硬件安全要求应符合 GB/T 34590.4-XXXX，6.4.2 中定义的安全机制的故障容错时间间隔，或者最大故障处理时间间隔。

注：硬件设计中能定义一种可能够控制故障，但不能满足容错时间间隔或最大故障处理时间间隔的机制。在这种情况下，进行本文件的第8章和第9章的定义的度量评估和ASIL等级分解时，不能考虑该机制。

6.4.8 硬件安全要求应符合按照 GB/T 34590.4-XXXX，6.4.2 中定义的多点故障探测时间间隔。

注 1：对于 ASIL 等级为 C 和 D 的安全目标来说，如果对应的安全概念没有描述明确的量值，多点故障探测时间间隔能定义为等于或小于该相关项从上电到下电的周期。

注 2：合适的多点故障探测时间间隔也能通过对随机硬件失效的发生概率的定量分析来确定（参见第 9 章）。

6.4.9 硬件安全要求应按照 GB/T 34590.8-XXXX 第 9 章的要求进行验证，以提供证据证明其：

a) 与技术安全概念、系统设计规范以及硬件规范的一致性；

b) 关于技术安全要求分配给硬件要素的完整性；

c) 与相关软件安全要求的一致性；及

d) 正确性与准确性。

6.4.10 在 GB/T 34590.4-XXXX，6.4.7 中最初定义的软硬件接口应被充分细化，以允许硬件被软件正确的控制和使用，并且应描述出硬件和软件之间的每一项安全相关的关联性。

6.4.11 软硬件开发人员应共同负责验证细化后的软硬件接口规范的充分性。

6.5 工作成果

6.5.1 硬件安全需求规范（包括测试和评估准则），由 6.4.1～6.4.8 的要求得出。

6.5.2 软硬件接口规范（细化的），由 6.4.10 的要求得出。

注：此工作成果可以参考GB/T 34590.6-XXXX 中6.5.2给出的相同的工作成果。

6.5.3 硬件安全要求验证报告，由 6.4.9 和 6.4.11 的要求得出。

7 硬件设计

7.1 目的

本章的目的是：

a) 创建一个硬件设计：

——支持以安全为导向的分析；

——考虑安全导向分析的结果；

——符合硬件安全要求；

——符合软硬件接口规范；

——符合系统架构设计规范；及

——满足所需的硬件设计特性；及

b) 定义在生产、运行、服务和报废期间的硬件功能安全要求并提供有关信息；及

c) 验证：

——硬件设计能满足硬件安全要求和软硬件接口规范；

——假设的有效性，此假设用于开发集成在已开发硬件中的每个 SEooC；及

——安全相关的特殊特性的适用性，以实现生产和服务期间的功能安全。

7.2 总则

硬件设计包括硬件架构设计和硬件详细设计。硬件架构设计表示所有的硬件组件以及它们彼此的相互关系。硬件详细设计是在电子电气原理图级别上，表示构成硬件组件的元器件间的相互连接。

为开发同时符合硬件安全要求及所有的非安全要求的唯一的硬件设计，在此子阶段，应在同一开发过程中处理安全和非安全性要求。

7.3 本章的输入

7.3.1 前提条件

应具备下列信息：

——硬件安全需求规范，按照 6.5.1；

——软硬件接口规范（细化的），按照 6.5.2；及

——系统架构设计规范，按照 GB/T 34590.4-XXXX，6.5.3。

7.3.2 支持信息

可能考虑下列信息：

——软件安全需求规范（参见 GB/T 34590.6-XXXX，6.5.1）；及

——非安全相关的硬件需求规范(来自外部)。

7.4 要求和建议

7.4.1 硬件架构设计

7.4.1.1 硬件架构应实现第 6 章定义的硬件安全要求。

7.4.1.2 硬件安全要求应分配到对应的硬件要素，因此，每个硬件要素都应按照分配给它的所有要求中最高的 ASIL 等级来开发。

注：硬件要素的各个特征将继承该要素所实现的硬件安全要求中最高的ASIL等级。

7.4.1.3 如果在硬件架构设计中对硬件安全要求应用了 ASIL 等级分解，ASIL 等级分解应按照 GB/T 34590.9-XXXX,第 5 章的要求进行。

7.4.1.4 如果一个硬件要素是由 ASIL 等级低于要素 ASIL 等级或没有指定 ASIL 等级的子要素组成，除非满足按照 GB/T 34590.9-XXXX，第 6 章的共存准则，否则应按照最高的 ASIL 等级处理每个子要素。

7.4.1.5 对硬件安全要求和硬件架构设计要素之间的可追溯性，应保持到硬件组件的最底层。

注：硬件安全要求的可追溯性不要求深入到硬件详细设计。对于不能划分为子元器件的硬件元器件，不分配硬件安全要求。例如，试图建立每个电容和电阻等硬件的可追溯性既没有意义，也没有益处。

7.4.1.6 为避免系统性故障，应通过使用表 1 中列出的原则，使硬件架构设计具有下述特性：

a) 模块化；

注：模块化使得硬件要素的设计无需修改就可以重复使用(如温度探测电路模块、微控制器中的ECC模块)。

b) 适当的粒度水平；及

注：其目的是架构在必要的详细程度上体现必要的信息，来显示安全机制的有效性。

c) 简单性。

表 1 硬件架构设计原则

原则		ASIL 等级			
		A	B	C	D
1	分层设计	+	+	+	+
2	安全相关硬件组件的精确定义接口	++	++	++	++
3	避免不必要的接口复杂性	+	+	+	+
4	避免不必要的硬件组件复杂性	+	+	+	+
5	可维护性（服务）	+	+	++	++
6	可测试性[a]	+	+	++	++
[a]可测试性包括开发，生产，服务和运行过程中的测试。					

7.4.1.7 在硬件架构设计时，应考虑安全相关硬件组件失效的非功能性原因，如果适用，可包括以下的影响因素：温度、振动、水、灰尘、电磁干扰、噪声因素、或来自硬件架构的其他硬件组件或其所在环境的串扰。

7.4.2 硬件详细设计

7.4.2.1 为了避免常见的设计缺陷，按照 GB/T 34590.2-XXXX，5.4.2.6，应运用相关的经验总结。

7.4.2.2 在硬件详细设计时，应考虑安全相关硬件元器件失效的非功能性原因，如果适用，可包括以下的影响因素：温度、振动、水、灰尘、电磁干扰、噪声因素、来自硬件组件的其他硬件元器件或其所在环境的串扰。

7.4.2.3 按照硬件详细设计，应考虑硬件元器件或硬件组件的任务剖面和运行条件，以确保硬件元器件或硬件组件在其规格范围内运行，以避免其由于预期使用而发生失效。

7.4.2.4 宜考虑鲁棒性设计原则。

注：鲁棒性设计原则可以通过硬件设计指南的应用来体现。

示例：关于组件应对环境和运行应力因素鲁棒性的保守规范。

7.4.3 安全分析

7.4.3.1 硬件设计的安全分析，应按照表 2 和 GB/T 34590.9-XXXX 第 8 章进行，以识别失效的原因和故障的影响。

注 1：安全分析的最初目的是支持硬件设计的定义，其后，安全分析能用于硬件设计验证（见 7.4.4）。

注 2：就安全分析支持硬件设计定义的目的来说，定性分析可能是适当且充分的。

表 2 硬件设计的安全分析

方法		ASIL 等级			
		A	B	C	D
1	演绎分析	o	+	++	++
2	归纳分析	++	++	++	++
分析的详细程度与设计的详细程度相对应。在某些情况下，两种方法都可在不同的细节层面上执行。					
示例：FMEA 是在硬件组件层面上完成的，它提供了在更高抽象层面上执行的 FTA 的基本事件。					

7.4.3.2 本要求适用于等级为 ASIL (B)、C 和 D 的安全目标。对于每个安全相关的硬件组件或元器件，针对所考虑的安全目标，安全分析应识别以下内容：

a) 安全故障；

b) 单点故障或残余故障；及

c) 多点故障（无论是可感知的、可探测的或潜伏的）。

注 1：识别多点故障的目的，并不要求对每一种可能的两个硬件故障的组合进行系统的分析，但至少要考虑从技术安全概念得出的组合（例如两个故障的组合：一个故障影响了安全相关的要素，另一个故障影响了相应的为达到或维持安全状态所需的安全机制）。

注 2：在大多数情况下，分析可能限制到双点故障。但有时阶次高于 2 的多点故障可能显示与技术安全概念有关（例如，当执行冗余安全机制时）。

7.4.3.3 本要求适用于等级为 ASIL（A）、(B)、C 和 D 的安全目标。应具备实施的安全机制对防止导致单点失效的故障或减少残余故障的有效性的证据。

为了这个目的：

a) 应具备证据以证明安全机制具有实现和保持安全状态的能力(特别是在容错时间间隔和最大故障处理时间间隔内适当的失效减轻能力）；及

b) 应评估由安全机制实现的残余故障的诊断覆盖率。

注 1：一个可能在任何时间（例如不仅在上电时）发生的故障，如果故障探测时间间隔加上相应安全机制的故障响应时间，大于相应的容错时间间隔或指定的最大故障处理时间间隔，则不能认为此故障被有效覆盖。

注 2：如果能证明某一特定故障模式可能仅发生上电时，并且在车辆行驶期间发生的概率是可以忽略的，那么对这些故障仅在上电后执行启动测试是可以接受的。

注 3：能用例如 FMEA 或 FTA 分析来构建理由。

注 4：根据对硬件要素失效模式和它们对更高层面的影响的认知，这种评估可能是硬件要素的整体诊断覆盖率，或更详细的失效模式的覆盖率评估。

注 5：附录 D 可以作为起始点，为已制定的安全机制确定诊断覆盖率。所声明的诊断覆盖率需要合适的理由支持（参见 GB/T 34590.10-XXXX 残余失效率评估条款和 GB/T 34590.11-XXXX 附录 A 中的示例）。

注 6：本要求适用于硬件、软件或两者结合实现的安全机制。

7.4.3.4 本要求适用于等级为 ASIL（A）、(B)、C 和 D 的安全目标。应具备实施的安全机制对防止潜伏故障的有效性的证据。

为了这个目的：

a) 应具备证据以证明安全机制在可接受的多点故障探测时间间隔内完成潜伏故障的失效探测和实现或保持安全状态及警示驾驶员的能力，以确定哪些故障保持潜伏，哪些故障可被探测到；及

b) 应评估由安全机制实现的潜伏故障的诊断覆盖率。

注 1：如果一个相应安全机制的故障处理时间间隔大于相应的潜伏故障的多点故障探测时间间隔，则不能认为此故障被有效覆盖。

注 2：能用例如 FMEA 或 FTA 分析来构建理由。

注 3：根据对硬件要素失效模式和它们对更高层面的影响的认知，这种评估可能是硬件要素的全局诊断覆盖率，或更详细的失效模式的覆盖率评估。

注 4：附录 D 可以作为起始点，为已制定的安全机制确定诊断覆盖率。所声明的诊断覆盖率需要合适的理由支持（参见 GB/T 34590.10-XXXX 残余失效率评估条款和 GB/T 34590.11-XXXX 附录 A 中的示例）。

注 5：本要求适用于硬件、软件或两者结合实现的安全机制。

7.4.3.5 如果适用，应按照 GB/T 34590.9-XXXX 第 7 章进行相关失效分析，提供证据证明设计中的硬件要素与它们的独立性要求相符合。

注 1：参见 GB/T 34590.9-XXXX，附录 C。

注 2：参见 GB/T 34590.11-XXXX，4.7。

7.4.3.6 如果硬件设计引入了新危害，且这个危害没有被现有的 HARA 报告覆盖，则应按照 GB/T34590.8-XXXX，第 8 章中的变更管理流程对它们进行引入和评估。

注：新识别出的、没有被现有安全目标覆盖的危害，通常是非功能性的危害。非功能性的危害在GB/T 34590范围之外，但在危害分析和风险评估中能对它们添加如下注释，“由于不在GB/T 34590的范围内，所以没有对该危害指定ASIL等级”。然而，也能指定一个ASIL等级作参考。

7.4.4 硬件设计的验证

7.4.4.1 应按照 GB/T 34590.8-XXXX 第 9 章来验证硬件设计，并按照表 3 中列出的硬件设计验证方法提供证据证明：

a) 满足硬件安全要求；

b) 与软硬件接口规范兼容；及

c) 用来在生产和服务过程中实现功能安全的安全相关特殊特性的适用性。

表 3 硬件设计验证

方法		ASIL 等级			
		A	B	C	D
1a	硬件设计走查[a]	++	++	o	o
1b	硬件设计检查[a]	+	+	++	++
2	安全分析	依照 7.4.3			
3a	仿真[b]	o	+	+	+
3b	通过硬件原型的开发[b]	o	+	+	+
该验证评审的范围是与硬件安全要求相关的技术正确性和完整性。					
[a]方法 1a 和 1b 检查硬件设计中硬件安全要求是否得到完整和正确的执行。 [b]当认为分析方法 1 和 2 不充分时，利用方法 3a 和 3b 检查硬件设计的特定点（例如 GB/T 34590.11-XXXX 4.8 中所述的故障注入）。					

7.4.4.2 在硬件设计过程中，如果发现任何硬件安全要求的实施是不可行的，应按照 GB/T 34590.8-XXXX 第 8 章中的变更管理流程提出变更请求。

7.4.4.3 应根据硬件安全要求和硬件设计规范验证用于开发集成到硬件中的 SEooC（独立于环境的安全要素）的假设的有效性。

7.4.5 生产、运行、服务和报废

7.4.5.1 如果安全分析表明安全相关的特殊特性与生产、运行、服务和报废相关，则应定义这些安全相关的特殊特性。安全相关的特殊特性的定义应包括：

a) 生产和运行的验证措施；及

b) 这些措施的接受准则。

示例：对一种依赖于新的传感器技术的硬件设计的安全分析（例如，影像或雷达传感器），能揭示出这些传感器与特殊安装流程的关系。这种情况下，在生产阶段对这些组件的额外验证措施可能是必要的。

7.4.5.2 如果安全相关硬件要素的错误组装、拆卸和报废可能对实现或维护功能安全产生不利影响，则应该将避免错误执行所需的信息告知按照 GB/T 34590.2-XXXX 第 7 章委任的负责生产、运行、服务和报废的人员。

7.4.5.3 按照 GB/T 34590.7-XXXX 5.4.1.2 和 5.4.3.3，安全相关硬件要素应可追溯，目的是：

a) 按照 GB/T 34590.2-XXXX 7.4.2.3 和 GB/T 34590.7-XXXX，7.4.1.1 进行有效的现场监测；及

b) 启用召回或更换管理。

注：这可能包括适当的标签或其他的硬件要素识别方法，来表示它们是与安全相关的。

7.4.5.4 如果错误的服务可能对实现或维护功能安全产生不利影响，则应该将避免此类影响执行所需的信息告知按照 GB/T 34590.2-XXXX 第 7 章委任的负责生产、运行、服务和报废的人员。

7.4.5.5 硬件设计过程中产生的硬件要素的生产、运行、服务和报废要求，应告知按照 GB/T 34590.2-XXXX 第 7 章委任的负责生产、运行、服务和报废的人员。

7.5 工作成果

7.5.1 硬件设计规范，由 7.4.1 和 7.4.2 的要求得出。

7.5.2 硬件安全分析报告，由 7.4.3 的要求得出。

7.5.3 硬件设计验证报告，由 7.4.4 的要求得出。

7.5.4 与生产、运行、服务和报废相关的需求规范，由 7.4.5 的要求得出。

8 硬件架构度量的评估

8.1 目的

本章的目的是提供基于硬件架构度量的证据，来证明相关项硬件架构设计在安全相关的随机硬件失效探测和控制方面的适用性。

8.2 总则

本章描述了两种硬件架构的度量，用于评估相关项架构应对随机硬件失效的有效性。

这些度量和关联的目标值在相关项层面对相关项的硬件要素进行评估，并与第9章描述的对随机硬件失效导致违背安全目标的评估互为补充。

这些度量所针对的随机硬件失效仅限于相关项中某些安全相关电子和电气硬件元器件，即那些能对安全目标的违背或实现有显著影响的元器件，并限于这些元器件的单点故障、残余故障和潜伏故障。对于机电硬件元器件，则仅考虑电气失效模式和失效率。

注 1：计算中能忽略阶次高于 2 的多点故障硬件要素，除非它们与技术安全概念相关。

硬件架构度量能在硬件架构设计和硬件详细设计过程中迭代使用。

硬件架构度量取决于相关项的整体硬件。对相关项涉及的每个安全目标，都应符合规定的硬件架构度量的目标值。

定义这些硬件架构度量以实现下列目标：

——客观上可评估：度量是用来区分不同的架构的一种可理解的手段；

——支持最终设计的评估（即基于选取的详细的硬件设计完成计算）；

——为评估硬件架构的充分性而提供基于 ASIL 等级的合格/不合格准则；

——显示用于防止硬件架构中单点或残余故障风险的安全机制的覆盖率是否足够（单点故障度量）；

——显示用于防止硬件架构中潜伏故障风险的安全机制的覆盖率是否足够（潜伏故障度量）；

——处理单点故障、残余故障和潜伏故障；

——考虑到硬件失效率的不确定性，确保硬件架构的鲁棒性；

——仅限于安全相关要素；及

——支持不同要素层面的应用，例如，能为供应商的硬件要素分配目标值。

示例：为方便分布式开发，能为集成电路或者 ECU 分配导出的目标值。

注 2：具有安全相关可用性要求的相关项（即，失去某一功能可能导致危害事件）与不具有安全相关可用性要求的相关项一样，受相同硬件架构度量的要求和目标的约束。

8.3 本章的输入

8.3.1 前提条件

应具备下列信息：

——硬件安全需求规范，按照 6.5.1；

——硬件设计规范，按照 7.5.1；及

——硬件安全分析报告，按照 7.5.2。

8.3.2 支持信息

可能考虑下列信息：

——技术安全概念（参见 GB/T 34590.4-XXXX，6.5.2）；及

——系统架构设计规范（参见 GB/T 34590.4-XXXX，6.5.3)。

8.4 要求和建议

8.4.1 本要求适用于等级为 ASIL (B)、C 和 D 的安全目标。应将按照附录 C 的诊断覆盖率、单点故障度量和潜伏故障度量的概念用于 8.4.2～8.4.9 的要求。

8.4.2 本要求适用于等级为 ASIL (B)、C 和 D 的安全目标。应结合残余故障和相关的潜伏故障来预估安全机制所实现的安全相关硬件要素的诊断覆盖率。

注 1：附录 D 可以作为起始点，为已制定的安全机制确定诊断覆盖率。所声明的诊断覆盖率需要合适的理由支持（参见 GB/T 34590.10-XXXX 残余失效率评估条款和 GB/T 34590.11-XXXX 附录 A 中的示例）。

注 2：根据对硬件要素失效模式和它们对更高层面影响的认知，这种评估可能是一个硬件要素的诊断覆盖率评估，或更详细的失效模式的覆盖率评估。

8.4.3 本要求适用于等级为 ASIL (B)、C 和 D 的安全目标。分析中用到的硬件元器件预估失效率的确定，应使用以下方法：

a) 使用业界公认的硬件元器件失效率数据；或

示例 1：用于确定硬件元器件失效率和失效模式分布的业界公认的来源包括 SN 29500, IEC 61709, MIL HDBK 217 F notice 2, RIAC HDBK 217 Plus, UTE C80-811, NPRD-2016, EN 50129:2003, Annex C, RIAC FMD-2016, MIL HDBK 338, 和 FIDES 2009 EdA。例如，能使用由“Alessandro Birolini-可靠性工程”定义的失效模式分布。

注 1：这些数据库给出的失效率数据一般都比较保守。

注 2：在应用选定的业界数据源时，为避免人为降低所计算出的基础失效率，应考虑以下因素:

——任务剖面;

——失效模式相对于运行条件的适用性;及

——失效率单位(每工作小时或每日历小时)。

b) 使用现场反馈的统计数据。这种情况下，预估的失效率宜有至少 70%的可比置信度；或

注 3：如果 SPFM 和 LFM 评估中使用的不同硬件元器件的故障率的置信度显著不同，则度量指标将是有偏差的。

注 4：在将这些从现场反馈的基于统计的数据与不同置信度的其他数据源的值一起使用之前，可能仍然需要衡量这些数据。也可见注释 7。

注 5：基于现场反馈的失效率能按照 GB/T 34590.8-XXXX 第 14 章(在用证明)的描述进行计算。

c) 使用工程方法形成的专家判断，该工程方法基于定量和定性的论证。应按照结构化准则进行专家判断，这些准则是判断的基础，应在失效率预估前进行设定。

注 6：考虑到设计的新颖性，专家判断的准则可能包括由现场数据、测试、可靠性分析和基于物理失效仿真方法的启发式信息组合。

注 7：能使用国际可靠性专家机构提供的资料:SAE J1211“鲁棒性验证”- 分析、建模和仿真提供了基于物理失效(PoF)的失效机制模型，JEDEC-JESD89，JEDEC-JESD91，JEDEC-JESD94 ，JEDEC-JEP143，JEDEC-JESD148。

注 8：如果失效率来自多个数据源(如在 8.4.3 列举的)结合，例如，如果不同部件的失效率不能从同一来源获得，则能使用比例系数来缩放失效率，以便不同失效率的预测质量相等。如果可获得两个失效率源之间的比例系数的原理，则能使用这种比例。

示例 2：只在一个数据源中发现要素失效率，而类似的要素在该源和另一个源中可用。比例系数是使用相同任务剖面的两个来源的失效率之比。

示例 3：数据手册的失效率通常被认为是保守的。如果已选择与使用手册数据一致的随机硬件失效目标值，则能通过应用适当的比例系数，使用从现场反馈的失效率(例如，对应于比通常更保守的置信度)。

注 9：如果没有合适的比例系数,则能将符合SPFM和LFM要求的单独目标值分配给所考虑的不同要素(类似于8.4.4)。

注 10：半导体指南参见 GB/T 34590.11-XXXX，4.6。

8.4.4 本要求适用于等级为 ASIL (B)、C 和 D 的安全目标。如果能够提供的硬件元器件失效率证据不足，应提出替代方案（例如，增加安全机制来探测和控制此故障）。如果替代方法仅包括附加的以下安全机制：

a) 对硬件元器件残余故障的诊断覆盖率应等于或高于相关项 SPFM 目标值；及

b) 对硬件元器件潜伏故障的诊断覆盖率应等于或高于相关项 LFM 目标值。

注 1：例如，充分的证据可以指失效率是通过 8.4.3 中列出的方法得到的。

注 2：在确定安全机制的覆盖率时，能考虑硬件元器件的安全故障比例。在这种情况下，覆盖率的计算与单点故障度量或潜伏故障度量的计算方法类似，都是在硬件元器件层面而不是在相关项层面进行的。

8.4.5 本要求适用于等级为 ASIL (B)、C 和 D 的安全目标。对于每一个安全目标，由 GB/T 34590.4-XXXX，6.4.5，要求的“单点故障度量（SPFM）”的定量目标值应基于下列参考目标值来源之一：

a) 来自应用于值得信赖的相似设计中，对硬件架构度量的计算；或

注 1：两个相似的设计有相似的功能和分配了相同 ASIL 等级的相似安全目标。

b) 来自表 4。

表 4 “单点故障度量”目标值的可能推导来源

	ASIL B	ASIL C	ASIL D

单点故障度量	≥90%	≥97%	≥99%

注 2：此定量目标的目的是提供：

——设计指南；及

——设计符合安全目标的证据。

8.4.6 本要求适用于等级为 ASIL（B）、C 和 D 的安全目标。对于每一个安全目标，由 GB/T 4590.4—XXXX 中的 6.4.5 要求的潜伏故障度量（LFM）的定量目标值应基于下列参考目标值来源之一：

a) 来自应用于值得信赖的相似设计中，对硬件架构度量的计算；或

注 1：两个相似的设计有相似的功能和分配了相同 ASIL 等级的相似安全目标。

b) 来自表 5。

表 5 “潜伏故障度量”目标值的可能推导来源

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

注 2：此定量目标的目的是提供：

——设计指南；及

——设计符合安全目标的证据。

8.4.7 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标，对于每个安全目标，相关项的整体硬件应符合下列两者之一：

a) 满足 8.4.5 中描述的“单点故障度量”目标值；或

b) 满足在硬件要素层面规定的合适目标，这些目标足以符合分配给相关项整体硬件的单点故障度量的目标值（如 8.4.5 中所描述的），并提供理由说明在硬件要素层面符合这些目标。

注 1：如果相关项包含失效率等级有显著差异的不同种类的硬件要素，就会存在这样的风险，即为了满足硬件架构度量时仅关注具有最高等级失效率的那些硬件要素。一个可能发生此情况的例子是：只考虑线束、保险丝或接插件的失效率，而忽略失效率显著较低的硬件元器件的失效率，就以为实现了对单点故障度量的符合性。为每一类硬件规定合适的度量目标有助于规避这种不良影响。

注 2：当瞬态故障与所用技术相关时，要考虑这些瞬态故障，能通过给它们指定并确认一个特定的“单点故障度量”目标值（如注 1 中说解释的），或通过一个基于对内部安全机制有效性验证的定性理由来处理这类瞬态故障。

注 3：如果不满足目标，将按 4.2 所述评估如何实现安全目标的理由。

注 4：能结合考虑多个或所有适用的安全目标来确定单点故障度量；但在这种情况下，采用最高 ASIL 等级的安全目标的度量目标。

示例：如果一个相关项由三个硬件要素 A，B 和 C 组成，失效率分别为λ_A， λ_B 和λ_C ，且 $\lambda_{total} = \lambda_A + \lambda_B + \lambda_C$，则满足以下公式要素 SPFM 目标值 $M_{SPFM,\ Element}$ 的元素的任意组合是可接受的：

$$\left(\frac{\lambda_A}{\lambda_{\text{total}}}\times M_{SPFM,\ A}+\frac{\lambda_B}{\lambda_{\text{total}}}\times M_{SPFM,\ B}+\frac{\lambda_C}{\lambda_{\text{total}}}M_{SPFM,\ C}\right)\geq M_{SPFM,Itemt\,\text{arg}et} \quad \text{.....(1)}$$

8.4.8 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。对于每个安全目标，相关项的整体硬件应该符合下列之一：

a) 满足 8.4.6 中描述的“潜伏故障度量”目标值；或

b) 满足在硬件要素层面规定的合适目标，这些目标足以符合分配给相关项整体硬件的潜伏故障度量的目标值（在 8.4.6 中给出），并有理由说明在硬件要素层面符合这些目标；或

c) 对于其故障可能导致安全机制（防止故障违背安全目标）无效的每个硬件要素，满足相关潜伏故障的诊断覆盖率目标值，该值与 8.4.6 中给出的潜伏故障度量目标值一致（被当作诊断覆盖率），当每个安全机制都是基于故障探测且其无效可能导致违背安全目标时，适用此选项。

注 1：选项 c）仅限于在每个相关项安全机制是基于故障探测的情况。在此情况下，通过这些安全机制的探测来警示目标功能的可能潜伏故障。在其他情况下，则只有选项 a)和 b)适用。

示例 1：附录 H 提供了考虑潜伏故障处理的不同类型安全机制的示例。

注 2：在选项 c）情况下，不计算度量，只评估安全机制对于硬件要素的潜伏故障的覆盖率。

注 3：如果相关项包含失效率等级显著差异的不同种类的硬件要素，就会存在这样的风险，即为了满足硬件架构度量时仅考虑具有最高等级失效率的那些硬件要素。一个可能发生此情况的例子是，只考虑线束、保险丝或接插件的失效率，而忽略失效率显著较低的硬件元器件的失效率，就认为实现了对潜伏故障度量的符合性。为每一类硬件规定合适的度量目标值有助于规避这种不良影响。

注 4：如果不满足目标，将按 4.2 所述评估如何实现安全目标的理由。

注 5：可以结合考虑多个或所有适用的安全目标来确定潜在故障度量；但在这种情况下，采用最高 ASIL 等级的安全目标的度量目标。

示例 2：如果一个相关项由三个硬件要素 A，B 和 C 组成，失效率分别为λ_A， λ_B 和λ_C ，且 $\lambda_{total} = \lambda_A + \lambda_B + \lambda_C$，则满足以下公式要素 LFM 目标值 $M_{LFM,\ Element}$ 的任意组合是可接受的：

$$\left(\frac{\lambda_A}{\lambda_{\text{total}}}\times M_{LFM,\ A}+\frac{\lambda_B}{\lambda_{\text{total}}}\times M_{LFM,\ B}+\frac{\lambda_C}{\lambda_{\text{total}}}M_{LFM,\ C}\right)\geq M_{LFM,Itemt\,\text{arg}et} \quad \text{(2)}$$

8.4.9 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。应按照 GB/T 4590.8-XXXX 第 9 章的要求，对应用 8.4.7 和 8.4.8 中的方法得出的结果进行验证评审，以提供其技术正确性和完整性的证据。

注：验证单点故障度量，确保只考虑了安全相关硬件要素的失效率，这样度量才不会受到不具备单点故障或残余故障可能性的、不必要的安全相关硬件要素的影响（例如，向安全机制添加了不必要的硬件要素）。

8.5 工作成果

8.5.1 相关项架构应对随机硬件失效的有效性分析，由 8.4.1～8.4.8 的要求得出。

8.5.2 相关项架构应对随机硬件失效的有效性评估的验证评审报告，由 8.4.9 的要求得出。

9 随机硬件失效导致违背安全目标的评估

9.1 目的

本章的目的是提供用于表明相关项随机硬件失效导致违背安全目标的残余风险足够低的证据。

注：“足够低”指“与已经在使用并且已知安全的相关项的残余风险相当”。

9.2 总则

推荐用两个可选的方法（见9.4）以评估违背安全目标的残余风险是否足够低。

两个方法都评估由单点故障、残余故障和可能的双点故障导致的违背安全目标的残余风险。如果显示为与安全概念相关，也能考虑多点故障。在分析中，对残余和双点故障，将考虑安全机制的覆盖率，并且，对双点故障也将考虑暴露持续时间。

9.4.2给出第一条方法的要求。“随机硬件失效概率度量”（PMHF）代表一种评估硬件要素随机失效是否违背所考虑的安全目标的定量分析方法。这种定量分析结果会与目标值作对比。

9.4.3给出第二条方法的要求。“对违背安全目标的每个原因进行评估”（EEC）是基于对每个硬件元器件及其在单点失效、残余失效和合理的双点失效方面对违背所考虑的安全目标的影响的独立评估。

所选用的方法在硬件架构设计和硬件详细设计中能被迭代应用。

本章的范围限于相关项的随机硬件失效。分析中所考虑的是电子电气硬件元器件。对于机电硬件元器件，仅考虑电气失效模式和失效率。

9.3 本章的输入

9.3.1 前提条件

应具备下列信息：

——硬件安全需求规范，按照 6.5.1；

——硬件设计规范，按照 7.5.1；及

——硬件安全分析报告，按照 7.5.2。

9.3.2 支持信息

可能考虑下列信息：

——技术安全概念（参见 GB/T 34590.4-XXXX，6.5.2）；及

——系统设计规范（参见 GB/T 34590.4-XXXX，6.5.3）。

9.4 要求和建议

9.4.1 总则

9.4.1.1 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。相关项应符合 9.4.2 或 9.4.3 中的一个。

9.4.1.2 本要求适用于等级为 ASILC 和 D 的安全目标。单一硬件元器件单点故障只有在提供有效论据证明其发生概率足够低时才能考虑接受，这些论据包括以下选项中的一个：

a) 采取专用措施；或

b) 对于 ASIL D 等级安全目标，需要满足以下准则：

——采用保守的数据来源；

——只有一小部分的失效率能够违背安全目标（例如：一个特殊的失效模式）；及

——得出的单点故障失效率小于失效率等级 1 对应失效率的十分之一（按照 9.4.3.3）。

c) 对于 ASIL C 等级安全目标，需要满足以下准则：

——采用保守的数据来源；

——只有一小部分的失效率能够违背安全目标（例如：一个特殊的失效模式）；及

——得出的单点故障失效率小于失效率等级 2 对应失效率的十分之一（按照 9.4.3.3）。

注 1：针对本条要求，能把一个微控制器，一个专用集成电路，或相似的系统级芯片看作硬件元器件。

注 2：专用措施可能包括：

a) 设计特征，如硬件元器件过设计（例如，电气或热应力等级）或者物理隔离（例如，印刷电路板上的触点间隔）；

b) 专门的来料抽样测试，以降低此失效模式发生的风险；

c) 老化测试；

d) 作为控制计划一部分的专用控制设备；及

e) 安全相关的特殊特性的分配。

9.4.1.3 本要求适用于等级为 ASIL C 和 D 的安全目标。如果一个硬件元器件的残余故障诊断覆盖率低于 90%，只有在提供有效论据证明其发生概率足够低时才能考虑接受，这些论据包括以下选项中的一个：

a) 采取专用措施（9.4.1.2 中注 2 列举的专用措施示例）；

b) 对于 ASIL D 等级安全目标，需要满足以下准则：

——采用保守的数据来源；

——只有一小部分的失效率能够违背安全目标（例如：一个特殊的失效模式）；及

——得出的残余故障失效率小于失效率等级 1 对应失效率的十分之一（按照 9.4.3.3）

c) 对于 ASIL C 等级安全目标，需要满足以下准则：

——采用保守的数据来源；

——只有一小部分的失效率能够违背安全目标（例如：一个特殊的失效模式）；及

——得出的残余故障失效率小于失效率等级 2 对应失效率的十分之一（按照 9.4.3.3）。

注 1：针对本条要求，能把一个微控制器，一个专用集成电路，或相似的系统级芯片看作硬件元器件。

注 2：当确定安全机制的覆盖率时，能考虑硬件元器件安全故障的比例。在这种情况下，覆盖率的计算与单点故障度量的计算类似，但仅在硬件元器件层面，而不在相关项层面。

9.4.1.4 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标，应按照 8.4.3 来估计在分析中用到的硬件元器件的失效率。

9.4.2 随机硬件失效概率度量（PMHF）的评估

9.4.2.1 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。9.4.2.2 或 9.4.2.3 要求的定量目标值应表述为相关项整个运行生命周期中每小时的平均概率。

注 1：即使共用相同单位，失效率和相关项整个运行生命周期中每小时的平均失效概率是不同的值。

注 2：运行生命周期仅包括实际工作时间。

9.4.2.2 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。应按照（GB/T34590.4-XXXX，6.4.5）的要求，为随机硬件失效在相关项层面导致违背每个安全目标的最大可能性定义定量目标值，使用来源 a）、b）或 c）的参考目标值，如下所列：

a) 来自表 6；或

b) 来自值得信赖的相似设计的现场数据；或

c) 来自应用于值得信赖的相似设计中的定量分析技术(使用按照 8.4.3 的失效率)。

注 1：这些来源于 a)、b）或 c）的定量目标值没有任何绝对的意义，仅有助于将一个新的设计与已有设计相比较。其目的是生成按照 9.1 描述的可用的设计指导，并获得设计符合安全目标的可用证据。

注 2：两个相似的设计拥有相似的功能和分配了相同 ASIL 等级的相似安全目标。

注 3：在没有其他来源的情况下，通常使用表 6 确定随机硬件失效的目标值。

注 4：表 6 中的值适用于单一系统构成的相关项（例如：发动机控制系统，电子稳定控制系统，电子助力转向系，安全气囊约束系统）。

注 5：表 6 中的目标值与手册的数据是保持一致的，是保守的。如果对由于随机硬件失效导致违背安全目标的评估是基于统计数据的（例如：来自现场数据），则能修改表 6 中给出的目标值，以避免为实现目标值而产生人为简化。

表 6 得出随机硬件失效目标值的可能来源

ASIL 等级	随机硬件失效目标值
D	<10-8h-1
C	<10-7 h-1
B	<10-7 h-1
此表中描述的定量目标值能按照4.2的规定进行剪裁以适应相关项的特定使用（例如：若相关项能在比一部乘用车典型使用时间更久的持续时间内才违背安全目标）。	

9.4.2.3 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。当一个相关项由多个系统构成时，根据 9.4.2.2 要求得出的目标值可以直接分配给构成该相关项的每一个系统。只要这些系统中的每一个都有可能违背相同的安全目标，并且相应的相关项目标值不会增加超过一个数量级，就可以应用此方法。

注 1：要求 9.4.2.3 中所述的可能性，例如，能用于新的更高级别功能所涉及的延用系统（例如，新 ADAS 功能使用的发动机管理系统、电子稳定控制系统、电动助力转向系统或气囊约束系统），并且这些系统在以前的开发中达到了同样的安全目标。

例如：如果一个等级为ASIL D的安全目标分配给由多个系统（最多10个）组成的相关项，其中每个系统都有可能违背该安全目标，则能将目标值10-8/h分配给组成该相关项的每个系统。

注 2：在附录 G 中给出了由两个系统组成的相关项 PMHF 预算分配的示例。

9.4.2.4 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。针对单点、残余和多点故障的硬件架构定量分析，应提供证据证明 9.4.2.2 或 9.4.2.3 要求的目标值已达到。此定量分析应考虑：

a) 相关项的架构；

b) 每个可导致单点故障或残余故障的硬件元器件的失效模式的估计失效率；

c) 每个可导致多点故障的硬件元器件的失效模式的估计失效率；

d) 安全机制对安全相关的硬件要素的诊断覆盖率；及

e) 多点故障情况下的暴露持续时间。

注 1：在定量分析中，考虑可能导致一个安全相关的硬件要素及其安全机制同时失效的硬件要素失效模式。它们可能是单点故障、残余故障或多点故障。

注 2：暴露持续时间从故障可能发生时开始，包括：

——与每个安全机制有关的多点故障探测时间间隔，或者当故障不对驾驶员显示（潜伏故障）时的车辆生命周期；

——单次行程的最长持续时间（对于驾驶员被要求以一种安全方式停车的情况）；及

——直到车辆进入车间维修前的平均时间间隔（对于驾驶员被警示要去维修车辆的情况）。

因此，暴露持续时间取决于涉及的监控类型（例如：连续监控、周期性自检、驾驶员监控、无监控）和探测到故障后的反应种类。对于连续监控触发向安全状态转移的情况，它可能短至几毫秒。当没有监控时，它可能长到车辆的生命周期。

对车辆去维修的平均时间的假设示例，取决于故障的类型：

——对舒适性功能的降级，200 次车辆行程；

——对驾驶辅助功能的降级，50 次车辆行程；

——对黄色警告灯或影响驾驶表现时，20 次车辆行程；

——对红色警告灯，1 次车辆行程。

通常不考虑维修所需要的时间（除了评估能暴露给维护人员的危害）。

一次车辆行程的平均时间间隔可能被认为等于：

——乘用车为 1 小时

——T&B 车辆为 10 小时

注 3：在大部分情况下，阶次高于二的多点失效对定量目标值的影响可以忽略。然而，在一些特定情况下（极高的失效率或差的诊断覆盖率），提供两个冗余的安全机制以达到目标可能是必要的。当技术安全概念是基于冗余的安全机制时，在分析中考虑阶次高于二的多点失效。

注 4：附录 D 可以作为起始点，为已制定的安全机制确定诊断覆盖率。所声明的诊断覆盖率需要合适的理由支持（参见 GB/T 34590.10-XXXX 残余失效率评估条款和 GB/T 34590.11-XXXX 附录 A 中的示例）。

注 5：如 9.4.2.2 注 1 中所指出的，PMHF 值不具有绝对意义，但对于比较新设计与现有设计是有用的。

注 6：如果 9.4.2.2 或 9.4.2.3 中定义的目标值没有被满足，应按 4.2 对给出的如何实现安全目标的论据进行评估。这种论据可能基于：

——识别影响 PMHF 值的主要因素和覆盖率较低的失效模式；及

——对这些因素进行评审，需考虑到其他准则的失效率、可靠性调查、诊断覆盖率、失效模式覆盖率、现场经验、验证措施、当前技术和专用措施（9.4.1.2 中的注 2 列出了专用措施的示例）。

附录F中给出了这些论据的示例。

注 7：基于对硬件要素失效模式及其在更高层面上后果的认知，评估可能是硬件要素的诊断覆盖率，或者更详细失效模式覆盖率的评估。

注 8：由于相关项 PMHF 值推导过程中的不确定性（例如，失效率、失效模式、失效模式分布、诊断覆盖率、安全故障比例的推导），计算值可能会有很大变化，解释时需特别注意。

9.4.3 对违背安全目标的每个原因进行评估(EEC)

9.4.3.1 对随机硬件失效导致违背安全目标的每个原因进行评估的方法，在图 3 和 4 的流程图中予以了阐明。使用故障发生准则对每个单点故障进行评估。使用综合了故障发生和安全机制有效性的准则对每个残余故障进行评估。

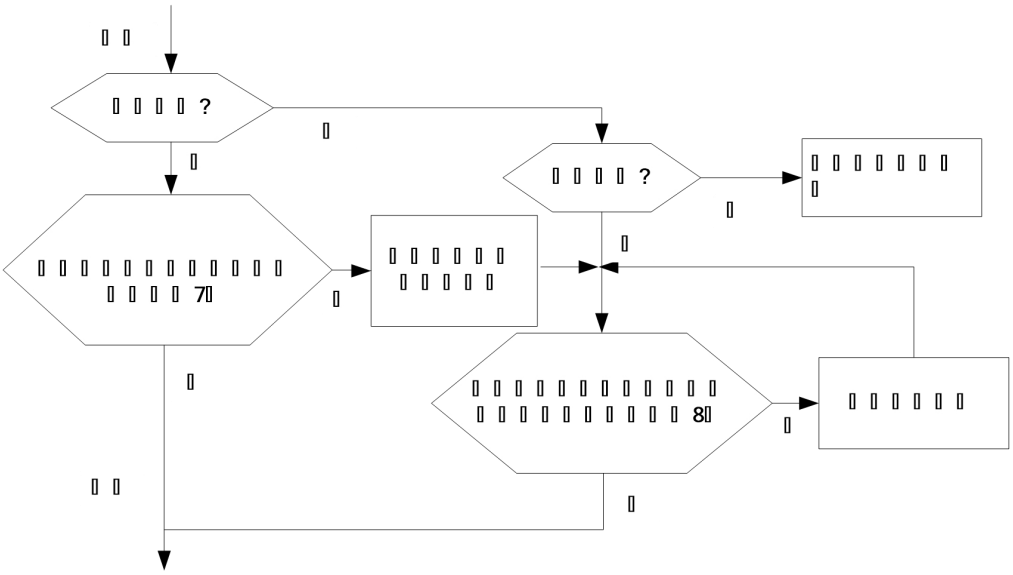


图 3 对单点和残余故障的评估流程

用于双点失效的流程在图4的流程图中进行了阐明。每个双点失效首先评估其可能性。如果两个故障同时导致的失效在足够短的时间内、以足够的覆盖率被探测或感知到，则认为这个双点失效不可能。如果双点失效是可能的，那么将使用综合了故障发生和安全机制覆盖率的准则对导致其发生的故障进行评估。

如果故障评估不满足故障发生和安全机制覆盖率的综合标准，则由故障导致的双点失效可能采用已有准则进行评估。

图3中描述的评估流程适用于硬件元器件（电阻，电容，CPU等）层面。

注：按照9.4.2.4的描述，通过定量分析技术（例如：FTA故障树分析，马尔科夫分析）评估双点失效的发生率。

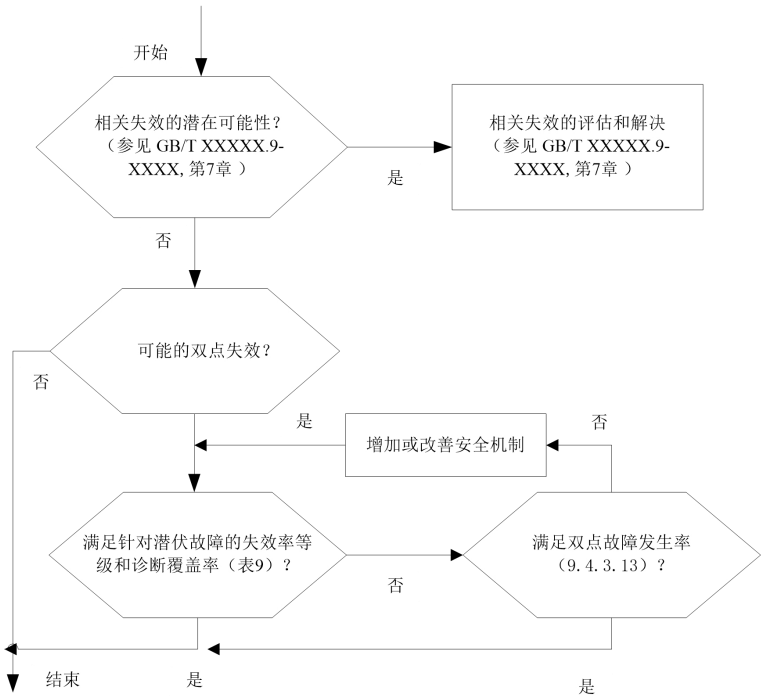


图 4 对双点失效的评估流程

9.4.3.2 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。对违背所考虑的安全目标的每个单点故障、残余故障和双点失效进行单独的评估，应在硬件元器件层面执行。此评估应按照要求 9.4.3.3 至 9.4.3.13 提供证据证明违背所考虑的安全目标的每个单点故障、残余故障和双点失效是可接受的。

注 1：此分析能被看作是对割集的评审，覆盖率的缺失或不完整被当作是故障。.

注 2：在大部分情况下，阶次高于二的多点失效是可忽略的。然而，在一些特定情况（极高的失效率或差的诊断覆盖率），提供两个冗余的安全机制可能是必要的。因此，当技术安全概念是基于冗余的安全机制时，在分析中考虑阶次高于二的多点失效是必要的。

注 3：当在子系统层面进行分析时，此分析能考虑在其他子系统中执行的系统安全机制。

注 4：如果不能按照要求 9.4.3.3 至要求 9.4.3.13 提供证据证明每个单点故障、残余故障和双点失效是可接受的，则按照 4.2 对满足该安全目标的合适理由进行评估。此理由能基于对这些故障/失效的评审，并考虑失效率、可靠性调查、诊断覆盖率、失效模式覆盖率、现场经验、验证措施、当前技术、以及专用措施等其他标准(9.4.1.2 注 2 给出了专用措施的示例）。

附录F给出了此类理由的示例。

9.4.3.3 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。硬件元器件失效率的失效率等级评级应按如下确定：

注 1：失效率等级 1、2 和 3 被引入以表示失效发生比率。这些等级分别与 FMEA 中使用的发生度水平 1、2 和 3 相似，即 1 分配给发生率最低的失效模式。

a) 失效率等级 1 对应的失效率应少于 ASIL D 等级的目标除以 100；除非应用 9.4.3.4；

注 2：能使用表 6 中给出的目标值。

b) 失效率等级 2 对应的失效率应小于或等于 10 倍的失效率等级 1 对应的失效率；

c) 失效率等级 3 对应的失效率应小于或等于 100 倍的失效率等级 1 对应的失效率；及

d) 失效率等级 i（i＞3）对应的失效率应少于或等于 $10^{(i-1)}$倍的失效率等级 1 对应的失效率。

注 3：失效率等级的分配是基于不考虑安全机制有效性的硬件元器件失效率。

注 4：对于元器件中的少数（如半导体器件的内部）的失效率高于失效率等级 i 上极限的情况，如果分配了等级 i 后元器件的平均失效率低于失效率等级 i 的上极限，则这些元器件能被分配等级 i。

9.4.3.4 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。如果给出理由说明失效率等级评级可除以一个不等于 100 的数字。在此情况下，应确保在同时考虑单点故障、残余故障和更高程度的割集时，保持了正确的评级。

示例：理由能基于最小割集的数量或安全相关的硬件要素的数量。

9.4.3.5 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。硬件元器件发生的单点故障应仅当相应的硬件元器件失效率等级符合表 7 给出的目标时，才被考虑接受。

表 7 针对单点故障的硬件元器件失效率等级目标

安全目标的 ASIL 等级	失效率等级
D	失效率等级 1 + 专用措施[a]
C	失效率等级 2 + 专用措施[a] 或 失效率等级 1
B	失效率等级 2 或 失效率等级 1
[a] 要求 9.4.1.2 的注 2 给出了专用措施的示例。	

注：当评估失效率等级时，能考虑硬件元器件的安全故障比例。

9.4.3.6 本要求适用于等级为 ASIL(B)、C 和 D 的安全目标。硬件元器件发生的残余故障应在失效率等级评级符合表 8 中为相应硬件元器件诊断覆盖率（针对残余故障）给出的目标时，被考虑接受。

注 1：所考虑的失效率是硬件元器件失效率，不考虑安全机制的有效性。

表 8 对给定的硬件元器件-残余故障诊断覆盖率的最大失效率等级

安全目标的 ASIL 等级	针对残余故障的诊断覆盖率			
	≥99.9%	≥99%	≥90%	<90%
D	失效率等级 4	失效率等级 3	失效率等级 2	失效率等级 1+ 专用措施[a]
C	失效率等级 5	失效率等级 4	失效率等级 3	失效率等级 2+ 专用措施[a]
B	失效率等级 5	失效率等级 4	失效率等级 3	失效率等级 2
[a] 要求 9.4.1.2 的注 2 给出了专用措施的示例。				

注 2：表 8 定义了给定目标 ASIL 等级允许的最大失效率等级和诊断覆盖率之间的关联。更低的失效率等级是可接受的，但不要求。

注 3：“更低的失效率等级”指带有更低数字的失效率等级。例如，针对失效率等级 3 的“更低的失效率等级”指失效率等级 2 和 1。

注 4：当确定安全机制的覆盖率时，能考虑硬件元器件安全故障的比例。在这种情况下，覆盖率的计算与单点故障度量的计算类似，但仅在硬件元器件层面，而不在相关项层面。

9.4.3.7 本要求适用于等级为 ASIL (B)，C 和 D 的安全目标。对失效率等级 i，i＞3，如果诊断覆盖率对于 ASIL D 等级大于或等于[100-$10^{(3-i)}$] %，或对于 ASIL B 和 C 等级大于或等于[100-$10^{(4-i)}$] %，则残余故障应被考虑接受。

注 1：所考虑的失效率是硬件元器件失效率，不考虑安全机制的有效性。

注 2：在确定安全机制的覆盖率时，能考虑硬件元器件安全故障的比例。在这种情况下，覆盖率的计算与单点故障度量的计算类似，但仅在硬件元器件层面，而不在相关项层面。

9.4.3.8 本要求适用于等级为 ASIL D 的安全目标。双点失效应被认为是可能的，如果：

a) 涉及到的两个硬件元器件中至少有一个，其拥有的诊断覆盖率（针对潜伏故障）低于 90%，或

b) 引起双点失效的双点故障中的一个，保持潜伏的时间长于 6.4.8 中规定的多点故障探测时间间隔。

注：在确定安全机制的覆盖率时，能考虑硬件元器件安全故障的比例。在这种情况下，覆盖率的计算与潜伏故障度量的计算类似，但仅在硬件元器件层面，而不在相关项层面。

9.4.3.9 本要求适用于等级为 ASIL C 的安全目标。双点失效应被认为是可能的，如果：

a) 涉及到的两个硬件元器件中至少有一个，其拥有的诊断覆盖率（针对潜伏故障）低于 80%；或

b) 引起双点失效的双点故障中的一个，保持潜伏的时间长于 6.4.8 中规定的多点故障探测时间间隔。

注：在确定安全机制的覆盖率时，能考虑硬件元器件安全故障的比例。在这种情况下，覆盖率的计算与潜伏故障度量的计算类似，但仅在硬件元器件层面，而不在相关项层面。

9.4.3.10 本要求适用于等级为 ASIL C 和 D 的安全目标。一个不可能的双点失效应被认为是与安全目标相符合的，因而是可接受的。

9.4.3.11 本要求适用于等级为 ASIL C 和 D 的安全目标。发生在硬件元器件中，并可能导致双点失效的双点故障，如果相应的硬件元器件符合表 9 中给出的失效率等级评级和诊断覆盖率（针对潜伏故障）的目标，应被认为是可接受的。

注 1：所考虑的失效率是硬件元器件失效率。因此，不考虑安全机制的有效性。

表 9 关于双点故障的硬件元器件失效率等级和覆盖率的目标

安全目标的 ASIL 等级	针对潜伏故障的诊断覆盖率		
	≥99%	≥90%	＜90%
D	失效率等级 4	失效率等级 3	失效率等级 2
C	失效率等级 5	失效率等级 4	失效率等级 3

注 2：表 9 定义了给定目标 ASIL 等级允许的最大失效率等级和能达到的诊断覆盖率水平。更低的失效率等级是可接受的，但不要求。

注 3：“更低的失效率等级”指带有更低数字的失效率等级。例如，针对失效率等级 3 的“更低的失效率等级”指失效率等级 2 和 1。

注 4：在确定安全机制的覆盖率时，能考虑硬件元器件安全故障的比例。在这种情况下，覆盖率的计算与潜伏故障度量的计算类似，但仅在硬件元器件层面，而不在相关项层面。

注 5：本要求同样适用于同一硬件元器件发生的可能导致双点失效的两个双点故障。

示例：安全机制“奇偶校验” 存在于硬件元器件“RAM”中，因此，影响双点失效的双点故障 “RAM 单元故障和奇偶校验安全机制故障” 都存在同一个硬件元器件 RAM 中。对于被视为可接受的两个双点故障，硬件部分"RAM"需要满足表 9 中所述的失效率等级和诊断覆盖率的目标。

9.4.3.12 本要求适用于等级为 ASIL C 和 D 的安全目标。对失效率等级 i，i＞3，针对 ASIL D 等级诊断覆盖率大于或等于[100-$10^{(4-i)}$] %，或针对 ASIL C 等级诊断覆盖率大于或等于[100-$10^{(5-i)}$] %，则双点故障可能导致的双点失效应认为是可接受的。

9.4.3.13 本要求适用于等级为 ASIL C 和 D 的安全目标。如果不能满足 9.4.3.11 或 9.4.3.12 的要求，则可能的双点失效应认为是可接受的，如果其发生的概率（以相关项在使用寿命内每小时的平均概率表示）小于或等于：

a) 针对安全目标 ASIL D 等级，失效率等级 1 的 1/10；及

b) 针对安全目标 ASIL C 等级，失效率等级 2 的 1/10。

9.4.4 验证评审

本要求适用于等级为ASIL(B)、C和D的安全目标。应对要求组9.4.2或9.4.3得出的分析进行验证评审，按照GB/T 34590.8-XXXX第9章提供其技术正确性和完整性的证据。

9.5 工作成果

9.5.1 由随机硬件失效导致违背安全目标的分析，由 9.4.2 或 9.4.3 的要求得出。

9.5.2 硬件专用措施的定义，如果需要，包括专用措施有效性的依据，由 9.4.1.2 和 9.4.1.3 的要求得出。

9.5.3 对随机硬件失效导致违背安全目标进行评估的验证评审报告，由 9.4.4 的要求得出。

10 硬件集成和验证

10.1 目的

本章的目的是确保所开发硬件符合硬件安全要求。

10.2 总则

本章所描述活动的目标是集成硬件要素，以验证硬件设计符合适当ASIL等级的硬件安全要求。

硬件集成和验证不同于GB/T 34590.8-2018第13章中硬件组件鉴定活动，该活动为硬件要素在符合GB/T 34590开发的相关项、系统或者要素中使用的适用性提供证明。

10.3 本章的输入

10.3.1 前提条件

应具备下列信息：

——硬件安全需求规范，按照 6.5.1；及

——硬件设计规范，按照 7.5.1。

10.3.2 支持信息

可能考虑下列信息：

——硬件安全分析报告（参见 7.5.2）。

10.4 要求和建议

10.4.1 硬件集成和验证活动应按照 GB/T 34590.8-2018 第 9 章执行。

10.4.2 硬件集成和验证应与 GB/T 34590.4-2018，7.4.1 中规定的集成规范与测试策略相协调。

注：如果已采用GB/T34590.9-2018第5章中定义的ASIL等级分解，已分解要素所对应的集成活动和其后的活动都要采用分解前的ASIL等级。

10.4.3 安全相关硬件元器件应按照基于国际质量标准或同等的公司标准而充分建立的完善流程进行鉴定。

示例：按照 ISO 16750、AEC-Q100 或 AEC-Q200，对电子元器件进行鉴定。

10.4.4 提供证据证明，对于选定硬件集成测试已定义适当的测试用例，测试用例应使用表 10 中所列方法的适当组合来导出。

表 10 导出硬件集成测试案例的方法

方法		ASIL 等级			
		A	B	C	D
1a	需求分析	++	++	++	++
1b	内部和外部接口分析	+	++	++	++
1c	等价类分析和生成[a]	+	+	++	++
1d	边界值分析[b]	+	+	++	++
1e	基于知识或经验的错误猜测法[c]	++	++	++	++
1f	功能的相关性分析	+	+	++	++
1g	相关失效的共有限制条件、次序及来源分析	+	+	++	++
1h	环境条件和操作用例分析	+	++	++	++
1i	现存标准[d]	+	+	+	+
1j	重要变量的分析[e]	++	++	++	++

[a] 为了高效导出必要的测试案例，可进行相似性分析。

[b] 例如，逼近或相交于边界（特定值之间）的值，和超出范围的值。

[c] 错误猜测测试基于经验教训，或者专家判断，或者两者结合所收集的数据。错误猜测可由 FMEA 支持。

[d] 现存标准包括 GB/T 28046 和 ISO 11452。

[e] 重要变量的分析包括最恶劣情况分析。

10.4.5 硬件集成和验证活动应当验证硬件安全要求实施的完整性和正确性。为了达到这些目的，应考虑表 11 所列方法。

表 11 验证硬件安全要求实施的完整性和正确性的硬件集成测试

方法		ASIL 等级			
		A	B	C	D
1	功能测试[a]	++	++	++	++
2	故障注入测试[b]	+	+	++	++
3	电气测试[c]	++	++	++	++

[a] 功能测试的目的是验证相关项的规范里定义的特性已经达到。将充分表征预期正常操作的数据输入到相关项，把它们的响应与规范里给定的响应做比较。对与规范不同的异常和规范不完整的迹象，应给予分析。

[b] 有关半导体组件故障注入的更多信息，请参考 GB/T 34590X,4.8

[c] 电气测试的目的是验证在规定的电压范围内(静态的和动态的)符合硬件安全要求。现有标准包括 ISO 16750 和 ISO 11452。

10.4.6 硬件集成和验证活动应验证硬件在环境和运行应力因素下的耐用性和鲁棒性。为了达到该目的，应考虑表 12 所列方法。

表 12 验证在应力下的耐用性，鲁棒性和运行的硬件集成测试

方法		ASIL 等级			
		A	B	C	D
1a	带基本功能验证的环境测试[a]	++	++	++	++
1b	扩展功能测试[b]	o	+	+	++
1c	统计测试[c]	o	o	+	++
1d	最恶劣情况测试[d]	o	o	o	+
1e	超限测试[e]	+	+	+	+
1f	机械测试[f]	++	++	++	++
1g	加速寿命测试[g]	+	+	++	++
1h	机械耐久测试[h]	++	++	++	++
1i	EMC 和 ESD 测试[i]	++	++	++	++
1j	化学测试[j]	++	++	++	++

[a] 在带基本功能验证的环境测试中，硬件安放于多种环境条件下进行硬件要求评估。可采用 GB/T 28046-4。

[b] 扩展功能测试检查相关项在极少发生（例如极端性能值）或者硬件规范之外（例如错误命令）的输入条件下的功能表现。在这些情况下，把观测到的硬件要素性能与特定要求进行比较。

[c] 统计测试的目的是，根据实际运行条件概况的预期统计分布，选定输入数据对硬件要素进行检测。定义验收准则，以便测试结果的统计分布能证明所要求的失效率。

[d] 最恶劣情况测试的目的是测试在最恶劣情况分析时发现的案例。在该测试中，调整环境条件至规范定义的最高允许余量值。检验硬件的相关反应并与特定要求相比较。

[e] 在超限测试中，把硬件要素置于环境或功能约束下，逐渐增加超过特定值直到硬件要素停止工作或者损坏。该测试的目的是确定要素在测试无故障时间所要求性能时鲁棒性的余量。

[f] 机械测试适用于机械特性，例如抗拉强度。可以应用 ISO 16750-3。

[g] 加速寿命测试的目标是通过将产品置于应力大于预期正常操作条件下，预测产品在使用寿命内，正常条件下产品的行为演化。加速测试是基于失效模式加速的分析模型。

[h] 这些测试的目的是研究要素能经受住的平均故障间隔期或者最大循环数。测试可以进行到失效发生或者损毁评估时为止。

[I] GB/T 21437.2、 GB/T 21437.3、ISO 11452-2 和 ISO 11452-4 适用于 EMC 测试；GB/T 19951 适用于 ESD 测试。

[j] ISO 16750-5 适用于化学测试。

10.5 工作成果

10.5.1 硬件集成和验证规范，由 10.4.1～10.4.6 的要求得出。

10.5.2 硬件集成和验证报告，由 10.4.1～10.4.6 的要求得出。

附 录 A

（资料性）

硬件层面产品开发的概览和工作流

表A.1提供了硬件层面产品开发特定阶段的目的、前提条件和工作成果的概览。

注：GB/T 34590.11为集成电路如何裁剪以下工作成果提供了指南。

表 A.1 硬件层面产品开发概览

章	目的	前提条件	工作成果
6 硬件安全要求的定义	a） 定义硬件安全要求。这些要求由技术安全概念和系统架构设计规范导出； b） 细化最初在GB/T 34590.4-XXXX,6.4.7中定义的软硬件接口规范；及 c） 验证硬件安全要求及软硬件接口规范与技术安全概念及系统架构设计规范的一致性。	——技术安全概念，按照GB/T 34590.4-XXXX，6.5.2； ——系统架构设计规范，按照GB/T 34590.4-XXXX，6.5.3；及 ——软硬件接口规范，GB/T 34590.4-XXXX，6.5.4。	6.5.1 硬件安全要求规范（包括测试和评估标准），由6.4.1～6.4.8的要求得出； 6.5.2软硬件接口规范（细化的），由6.4.10的要求得出； 6.5.3硬件安全要求验证报告，由6.4.9和6.4.11的要求得出。
7 硬件设计	a） 创建一个硬件设计： ——支持以安全为导向的分析； ——考虑安全导向分析的结果； ——符合硬件安全要求； ——符合软硬件接口规范； ——符合系统架构设计规范；及 ——满足所需的硬件设计特性；及 b） 在生产、运行、服务和报废期间定义硬件要求并提供有关硬件功能安全的信息；及c）验证： ——硬件设计能满足硬件安全要求和软硬件接口规范； ——假设的有效性，此假设用于开发集成在已开发硬件中的每个SEooC；及 ——安全相关的特殊特性的适用性，使在生产和服务过程中实现功能安全。	——硬件安全需求规范，按照6.5.1； ——软硬件接口规范（细化的），按照6.5.2；及 ——系统架构设计规范，按照GB/T 34590. 4-XXXX，6.5.3。	7.5.1 硬件设计规范，由7.4.1和7.4.2的要求得出； 7.5.2 硬件安全分析报告，由7.4.3的要求得出； 7.5.3 硬件设计验证报告，由7.4.4要求得出； 7.5.4 与生产、运行、服务和报废相关的需求规范，由7.4.5的要求得出。
8 硬件架构度量的评估	提供基于硬件架构度量的证据，来证明相关项硬件架构设计在安全相关的随机硬件失效探测和控制方面的适用性。	——硬件安全需求规范，按照6.5.1； ——硬件设计规范，按照7.5.1；及 ——硬件安全分析报告，按照7.5.2。	8.5.1 相关项架构应对随机硬件失效的有效性分析，由8.4.1～8.4.8的要求得出； 8.5.2 相关项架构应对随机硬件失效的有效性评估的验证评审报告，由8.4.9要求得出。

9 随机硬件失效导致违背安全目标的评估	提供用于表明相关项随机硬件失效导致违背安全目标的残余风险足够低的证据。注:“足够低”指“与已经在使用并且已知安全的相关项的残余风险相当”。	——硬件安全需求规范，按照6.5.1； ——硬件设计规范，按照7.5.1；及 ——硬件安全分析报告，按照7.5.2。	9.5.1 随机硬件失效导致违背安全目标的分析，该失效由9.4.2或9.4.3的要求得出； 9.5.2 硬件专用措施规范，如果需要，包括由第9.4.1.2条和9.4.1.3条要求得出的专用措施有效性的依据； 9.5.3 对随机硬件失效导致违背安全目标进行评估的验证评审报告，由9.4.4的要求得出。
10 硬件集成和测试	确保所开发硬件符合硬件安全要求。	——硬件安全需求规范，按照6.5.1；及 ——硬件设计规范，按照7.5.1。	10.5.1 硬件集成和验证规范，由10.4.1～10.4.6的要求得出； 10.5.2 硬件集成和验证报告，由10.4.1～10.4.6的要求得出。

附 录 B

（资料性）

硬件要素的失效模式类别

硬件要素的失效模式能按图B.1所示分类。图B.2中的流程图说明了如何将硬件要素的一个失效模式归入到这些类别中的某一个。

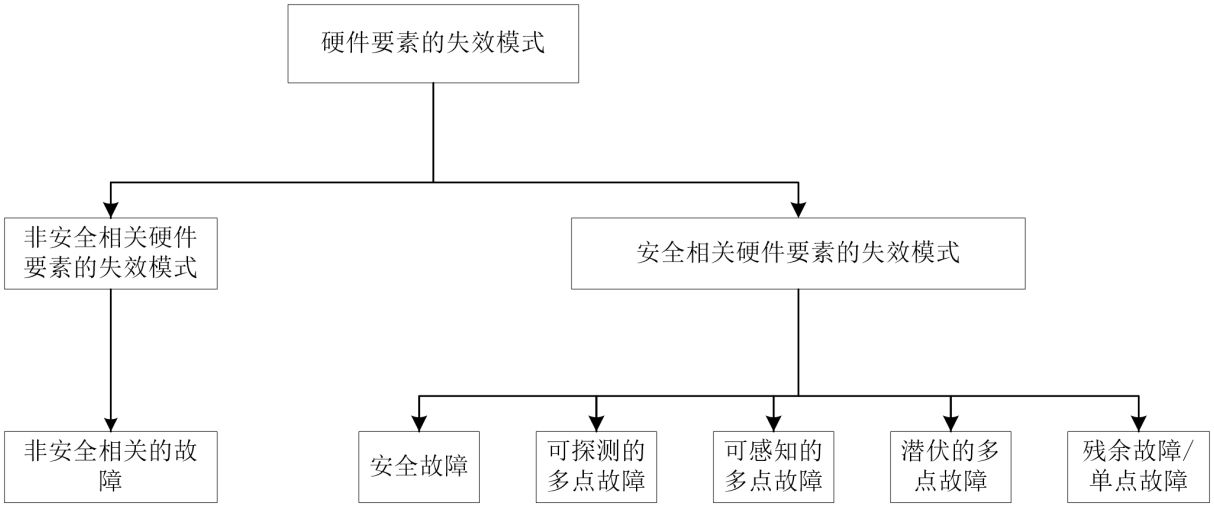


图 B.1 硬件要素的失效模式类别

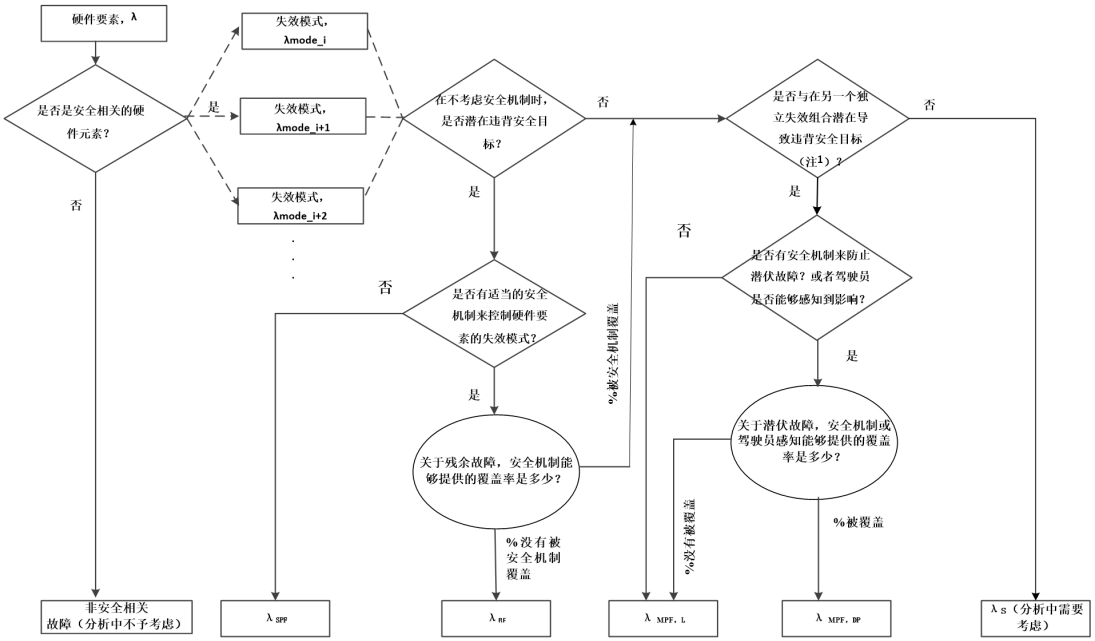


图 B.2 失效模式分类流程图示例

注 1：有些要素的失效不会显著增加违背安全目标的概率，能从分析中去除这些要素并将其失效模式归入安全故障，例如，n 阶（n>2）的多点故障可被认为是安全故障，除非在技术安全概念中表明其是相关的。

示例：在缺乏安全机制的情况下，硬件要素的失效模式中潜在违背安全目标的部分，若由两个独立的安全机制所覆盖，能看作是 3 阶的多点故障。它能被认为是安全的，除非安全概念中表明其是相关的。

注 2：在考虑不同的安全目标时，同一故障可能被归入不同的类别。

附 录 C

（规范性）

硬件架构度量

C.1 故障分类和诊断覆盖率

C.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。

示例：n 阶（n>2）的多点故障的硬件要素能在计算中排除，除非在技术安全概念中明确表明相关。

C.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

示例 1：硬件要素可能有“开路”，“对地短路”，“短路接高”故障，但是只有“开路”和“对地短路”的故障被安全机制所覆盖。如果“短路接高”故障导致违背了特定安全目标，且没有被安全机制所覆盖，那么它是一种残余故障。

c) 多点故障;或

注 1：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C.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：

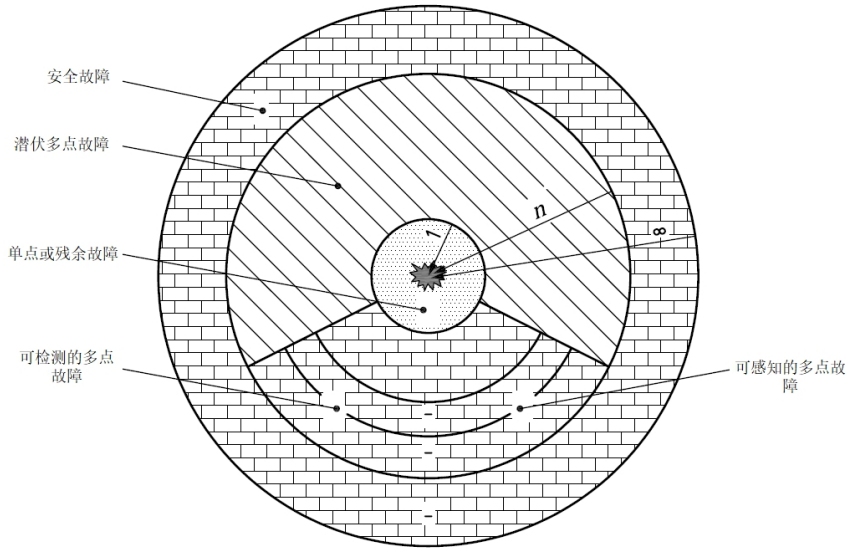


图 C.1 相关项中与安全相关的硬件要素的故障分类

在该图示中：

——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)；

——距离等于 n 的故障位于圆环 n 和 n-1 之间的区域；及

——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。

注 2：就瞬态故障而言，如果针对此故障的安全机制可将相关项修复为无故障状态，这样的故障可能被考虑为可探测的多点故障，即使驾驶员从未被告知故障的存在。

示例 2：在使用一个纠错码去保护存储空间以应对瞬态故障的情况下，如果安全机制（除向中央处理器提供一个正确值外）修复了存储阵列中发生翻转的位（例如，通过回写一个正确的值），相关项被修复为一个无故障状态。

因此每个安全相关硬件要素的失效率λ，都能按照等式(C.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：

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

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(C.2)来表述，如下：

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

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(C.3)提供了一个关于残余故障的失效率的保守估算。

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

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。

注 3：当已知失效模式分布和失效模式覆盖率时，λ_{RF}能按如下方式计算：

$$\lambda_{RF} = \sum_{\mathrm{alli}} \lambda \times D_{FMI,\,SR} \times \left(1 - F_{FM\mathrm{i},\,\mathrm{safe}}\right) \times F_{FM\mathrm{i},\,\mathrm{PVSG}} \times \left(1 - K_{FMC\mathrm{i},\,RF}\right) \quad (C.4)$$

式中：

$\lambda \times D_{FMi,SR}$ —— 安全相关硬件要素的第i个失效模式的失效率；

$F_{FMi,safe}$ —— 第i个失效模式中被认为是安全的故障占比；

$(1 - F_{FMi,safe}) \times F_{FMi,PVSG}$ —— 在缺乏安全机制的情况下，第i个失效模式中潜在直接违背安全目标的故障占比；

$K_{FMCi,RF}$ —— 第i个失效模式相对于残余故障的失效模式覆盖率。

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(C.5)提供了关于潜伏故障的失效率的保守估算：

$$\lambda_{MPF,\,L} \le \lambda_{MPF,\,L,\,\mathrm{est}} = \lambda \times \left(1 - \frac{K_{DC,\,MPF,\,L}}{100\%}\right) \quad (C.5)$$

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 4：当已知失效模式分布和失效模式覆盖率时，$\lambda_{MPF,\,L}$能按如下方式计算：

$$\lambda_{MPF,L}=\sum_{\text{alli}}\lambda\times D_{FM\text{i},SR}\times\left(1-F_{FM\text{i},\text{safe}}\right)\times\left[F_{FM\text{i},PVSG}\times K_{FMC\text{i},RF}+\left(1-F_{FM\text{i},\text{PVSG}}\right)\right]\times\left(1-K_{FMC\text{i},MPF}\right) \quad (C.6)$$

式中：

$\lambda\times D_{FMi,SR}$ —— 安全相关硬件要素的第i个失效模式的失效率；

$F_{FMi,safe}$ —— 第i个失效模式中被认为安全的故障占比；

$(1-F_{FMi,safe})\times F_{FMi,PVSG}$ —— 在缺乏安全机制的情况下，第i个失效模式中潜在直接违背安全目标的故障占比；

$(1-F_{FMi,safe})\times(1-F_{FMi,PVSG})$ —— 第i个失效模式中不认为是安全的，但在缺乏安全机制的情况下，也不会潜在直接违背安全目标的故障占比；

$K_{FMCi,RF}$ —— 对于残余故障，第i个失效模式的失效模式覆盖率；

$K_{FMCi,MPF}$ —— 对于潜伏故障，第i个失效模式的失效模式覆盖率。

注 5：针对这个目的，附录 D 能作为声明 DC 有合适理由支持诊断覆盖率的基础。

注 6：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。附录 B 描述了用于故障分类的流程图。

C.2 单点故障度量

C.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。

C.2.2 本要求适用于等级为ASIL (B)、C和D的安全目标。等式(C.7)中的计算应用于确定单点故障度量：

$$1-\frac{\sum_{SR,\,HW}\left(\lambda_{SPF}+\lambda_{RF}\right)}{\sum_{SR,\,HW}\lambda}=\frac{\sum_{SR,\,HW}\left(\lambda_{MPF}+\lambda_{S}\right)}{\sum_{SR,\,HW}\lambda} \quad (C.7)$$

式中：

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

注 1：该度量仅考虑相关项中与安全相关硬件要素。

示例：n 阶（n>2）的全部安全的故障或多点故障的硬件要素可在计算中排除，除非在技术安全概念中明确表明相关。

注 2：图 C.2 给出了单点故障度量的图示。

注 3：附录 E 给出了计算“单点故障度量”的示例。

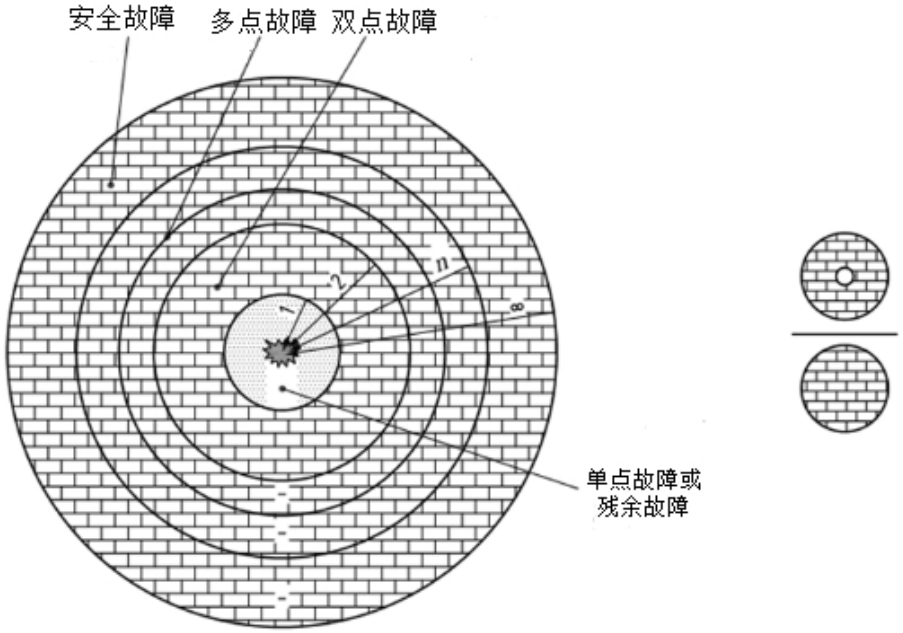


图 C.2 单点故障度量的图示

C.3 潜伏故障度量

C.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。

C.3.2 本要求适用于等级为ASIL(B)、(C)和D的安全目标。等式(C.8)中的计算应用于确定潜伏故障度量：

$$1-\frac{\sum_{\mathrm{SR,HW}}(\lambda_{\mathrm{MPF,L}})}{\sum_{\mathrm{SR,HW}}(\lambda-\lambda_{\mathrm{SPF}}-\lambda_{\mathrm{RF}})}=\frac{\sum_{\mathrm{SR,HW}}(\lambda_{\mathrm{MPF,DP}}+\lambda_{\mathrm{S}})}{\sum_{\mathrm{SR,HW}}(\lambda-\lambda_{\mathrm{SPF}}-\lambda_{\mathrm{RF}})} \qquad (C.8)$$

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 4：该度量仅考虑相关项中与安全相关硬件要素。

示例：n 阶（n>2）的全部安全的故障或多点故障的硬件要素可在计算中排除，除非在技术安全概念中明确表明相关。

注 5：图 C.3 给出了潜伏故障度量的图示。

注 6：附录 E 给出了计算“潜伏故障度量”的示例。

注 7：对于实现容错以满足安全相关可用性要求的相关项潜伏故障度量，识别出 2 阶以上的多点故障非常重要。这能适用于主系统故障后冗余系统长期运行的冗余系统潜伏故障。

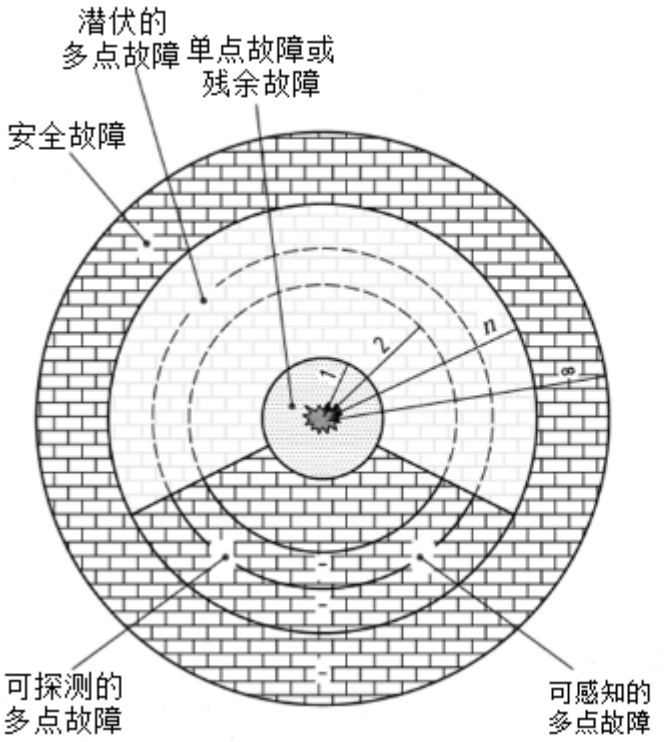


图 C.3 潜伏故障度量的图示

附 录 D

（资料性）

诊断覆盖率的评估

D.1 总则

此附录的目的是：

a) 诊断覆盖率的评估，为以下两方面提供理由：

1) 符合第 8 章给出的单点故障度量和潜伏故障度量；

2) 符合第 9 章定义的由于随机硬件失效导致违背安全目标的评估；

b) 对合适的安全机制进行选择的指南，这些安全机制在电气/电子架构中探测要素的失效。

图 D.1 表示常见的嵌入式系统的硬件。表 D.1 列举了这个系统中硬件要素的典型失效模式。表的最左一列是每个要素，要素的右侧则是其对应的一个或多个失效模式。表中没有穷尽所有的失效模式，可以根据其他已知的失效模式或实际应用做调整。

这些与要素故障相关的安全机制的更多细节参考表 D.2 到 D.10 各行。对于给定要素的典型安全机制的有效性，按照它们对所列举的失效模式覆盖能力进行了分类，分别为低、中或高诊断覆盖率。这些低，中或高的诊断覆盖率被分别对应为 60%、90%或 99%的典型覆盖水平。

对失效模式及其相应的安全机制的指定，根据下列条件可与表 D.1 中不同：

a) 被诊断探测到的失效模式的来源不同；

b) 安全机制的有效性；

c) 安全机制的特定实现；

d) 安全机制（周期性）的执行时序；

e) 在系统中使用的硬件技术；

f) 基于系统中硬件的失效模式的概率；及

g) 失效模式及其不同覆盖率水平的失效模式子类的更详细分析。

总之，表 D.1 提供了指南，该指南可基于对系统要素的分析而进行修改。这些指南不针对安全概念中为避免违背安全目标而定义的特定限制。当评估常见典型诊断覆盖率时，安全机制不考虑这些限制，例如时序方面（诊断周期）。但评估特定诊断覆盖率时，相关项中用于避免违背安全目标的安全机制将考虑这些限制。

示例：在本附录，一个安全机制可具有高的常见典型诊断覆盖率。但是，如果使用的诊断测试时间间隔长于所需的诊断测试时间间隔（为满足相关故障的容错时间间隔），那么针对避免违背安全目标所设定的诊断覆盖率将大幅降低。

因此表 D.2 到 D.10 可以被视为评估这些安全机制诊断覆盖率的起点，同时，这些声明的诊断覆盖率要有恰当的理由支持（例如，使用故障注入方法或分析论据）。另外，所给信息用于定义要素失效模式；然而，相关的失效模式最终依赖于要素应用场合。

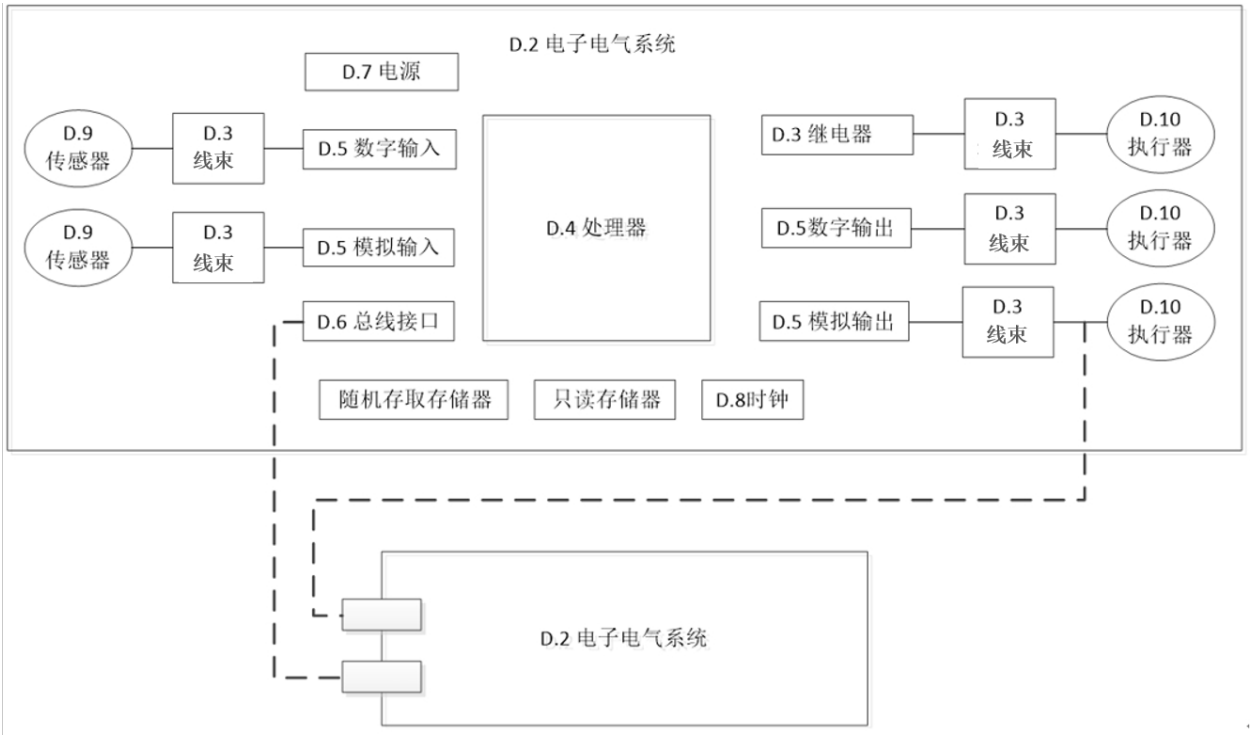


图 D.1　常见系统硬件

为了支撑表 D.1 的信息，表 D.2 到 D.10 给出了诊断测试技术的指导准则。D.1 到 D.10 并未穷尽所有诊断测试技术，只要有证据支持声明的诊断覆盖率，也能采用其他技术。如果证明上述技术合理，不管是简单还是复杂的要素，都可预估为更高的、甚至 100%的诊断覆盖率。

表 D.1　失效模式分析

要素	参考表格	已分析的失效模式
总体要素		
电气/电子系统	D.2 电气/电子系统	-无通用的失效模式可用 -需要详细分析
电气要素		
继电器	D.3 电气要素	-不通电或不断电 -单个触点熔接
线束，含接头和连接器		-开路 -接触电阻 -短接到地（直流耦合） -短接到电源 -相邻插针间短接 -插针之间的电阻漂移
传感器，含信号开关	D.9 传感器	-需要详细分析 -应覆盖的典型的失效模式包括： 超出范围 偏差

		卡滞在范围内 震荡 -集成传感器和转换器，见 GB/T 34590.11-XXXX，5.5
执行端要素（执行器、灯、蜂鸣器、显示屏等等）	D.10 执行器	-无通用的失效模式可用 -需要详细分析
常规半导体要素		
电源	D.7 电源	-漂移和振荡 -欠压和过压 -电源尖峰 见 GB/T 34590.11-XXXX，5.2
时钟	D.8 程序序列监控/时钟	-不正确的频率 -抖动 见 GB/T 34590.11-XXXX，5.2
非易失性存储器	GB/T 34590.11-XXXX，表 32	见 GB/T 34590.11-XXXX，5.1,表 29
易失性存储器	GB/T 34590.11-XXXX，表 33	见 GB/T 34590.11-XXXX，5.1,表 29
数字输入/输出	D.5 模拟和数字输入/输出	不正确的输入/输出 见 GB/T 34590.11-XXXX，5.1,表 30
模拟输入/输出		不正确的输入/输出 见 GB/T 34590.11-XXXX，5.2,表 36
处理单元	D.4 处理单元/D.8 可编程序列监控/时钟	不正确的输出 见 GB/T 34590.11-XXXX，5.1,表 30
通信		
数据传输 （按照 GB/T 34590.6-XXXX, D.2.4 条进行分析）	D.6 通信总线（串行，并行）	-通信节点丢失 -消息损坏 -消息不可接受的延时 -消息丢失 -非预期的消息重复 -消息顺序错误 -消息插入 -消息伪装 -消息寻址错误

注 1：相关的失效模式和故障模型是根据具体情况确定的，通常取决于所使用的技术和实现情况。详细的半导体故障模型见 GB/T 34590.11-XXXX，4.3.1。例如：如果一个要素的失效模式为 x、y 和 z，失效模式分布为 X、Y 和 Z，则有效诊断覆盖率计算如下：

$KDC = X \times KFMC,x + Y \times KFMC,y + Z \times KFMC,z$

式中：

KDC ——硬件要素的诊断覆盖率；

X ——失效模式 x 的失效模式分布；

KFMC,x——x 失效模式的失效覆盖率；

Y ——失效模式 y 的失效模式分布；

KFMC,y——y 失效模式的失效覆盖率；

Z ——失效模式 z 的失效模式分布；

KFMC,z——z 失效模式的失效覆盖率；及

X + Y + Z = 100 %

注 2：半导体的故障模型、失效模式与相关分布的关系见 GB/T 34590.11-XXXX, 4.3。

表 D.2 电气/电子系统

安全机制/措施	见技术概览	可实现的典型诊断覆盖率	备注
通过在线监控进行失效探测	D.2.1.1	低	取决于失效探测的诊断覆盖率。
比较器	D.2.1.2	高	取决于比较的质量。
多数表决电路	D.2.1.3	高	取决于表决的质量。
动态性原则	D.2.2.1	中	取决于失效探测的诊断覆盖率。
数字信号的模拟监控	D.2.2.2	低	—
两个独立单元间的软件交叉自检	D.2.3.3	中	取决于自检的质量。

表 D.3 电气要素

安全机制/措施	见技术概览	可实现的典型诊断覆盖率	备注
通过在线监控进行失效探测	D.2.1.1	高	取决于失效探测的诊断覆盖率。
注：该表格仅涉及专用于电气要素的安全机制。通用技术，如基于数据的比较（见 D.2.1.2），也能用来探测电气要素的失效，但没有集成到该表中（已经包含在表 D.2 电气/电子系统中）。			

注：下述列表讨论了主要用于系统层面组件的安全机制。GB/T 34590.11-XXXX 中描述了更多关于可集成在组件中的安全机制：

——5.1 数字组件；

——5.2 模拟和混合信号组件；

——5.3 可编程逻辑器件；

——5.4 多核组件；及

——5.5 传感器和转换器。

表 D.4 处理单元

安全机制/措施	见技术概览	可实现的典型诊断覆盖率	备注
通过软件进行自检：有限模式（单通道）	D.2.3.1	中	取决于自检的质量。
两个独立单元间的软件交叉自检	D.2.3.3	中	取决于自检的质量。
硬件支持的自检（单通道）	D.2.3.2	中	取决于自检的质量。
软件多样化冗余（单硬件通道）	D.2.3.4	高	取决于多样化质量。共模失效会降低诊断覆盖率。
通过软件进行相互比较	D.2.3.5	高	取决于比较的质量。
硬件冗余（例如：双核锁步、非对称冗余、编码处理）	D.2.3.6	高	取决于冗余质量。共模失效会降低诊断覆盖率。
配置寄存器测试	D.2.3.7	高	仅配置寄存器。
堆栈上溢出/下溢出探测	D.2.3.8	低	仅堆栈边界测试。
集成硬件一致性监控	D.2.3.9	高	仅覆盖非法硬件异常。
注：该表格仅涉及专用于处理单元的安全机制。通用技术，如基于数据的比较（见 D.2.1.2），也能用来探测电气要素的失效，但没有集成到该表中（已经包含在表 D.2 电气/电子系统中）。			

表 D.5 模拟和数字输入/输出

安全机制/措施	见技术概览	可实现的典型诊断覆盖率	备注
通过在线监控进行失效探测（数字输入/输出）[a]	D.2.1.1	低	取决于失效探测的诊断覆盖率。
测试模式	D.2.4.1	高	取决于模式类型。

数字输入/输出的编码保护	D.2.4.2	中	取决于编码类型。
多通道并行输出	D.2.4.3	高	—
受监控的输出	D.2.4.4	高	仅当数据流的改变出现在诊断测试的间隔内。
输入比对/表决（1oo2、2oo3或者更好的冗余）	D.2.4.5	高	仅当数据流的改变出现在诊断测试的间隔内。
[a] 数字输入/输出可以是周期性的。			

表 D.6　通信总线（串行，并行）

安全机制/措施	见技术概览	可实现的典型诊断覆盖率	备注
一位硬件冗余	D.2.5.1	低	—
多位硬件冗余	D.2.5.2	中	—
回读已发送的消息	D.2.5.9	中	—
完全硬件冗余	D.2.5.3	高	共模失效模式会降低诊断覆盖率。
使用测试模式检验	D.2.5.4	高	—
发送冗余	D.2.5.5	中	取决于冗余类型，只对瞬态故障有效。
信息冗余	D.2.5.6	中	取决于冗余类型。
帧计数器	D.2.5.7	中	—
超时监控	D.2.5.8	中	—
信息冗余、帧计数器和超时监控的组合	D.2.5.6、D.2.5.7 和 D.2.5.8	高	对于没有硬件冗余和测试模式的系统，这些安全机制的组合可以声明达到高覆盖率。

表 D.7　电源

安全机制/措施	见技术概览	可实现的典型诊断覆盖率	备注
电压或电流控制（输入）	D.2.6.1	低	—
电压或者电流控制（输出）	D.2.6.2	高	—

表 D.8　程序序列监控/时钟

安全机制/措施	见技术概览	可实现的典型诊断覆盖率	备注
具有独立时间基准，无时间窗口的看门狗	D.2.7.1	低	—
具有独立时间基准和时间窗口的看门狗	D.2.7.2	中	取决于时间窗口的时间限制。
程序序列的逻辑监控	D.2.7.3	中	只有当外部暂时事件影响逻辑程序流的时候才能有效预防时钟失效。提供了可能导致软件运行次序紊乱的内部硬件失效（比如中断频率错误）的覆盖率。
对程序序列的时间和逻辑监控的组合	D.2.7.4	高	—
基于时间的程序序列的时间和逻辑联合监控	D.2.7.5	高	提供了对可能导致软件运行序列紊乱的内部硬件失效的覆盖。 当采用非对称设计时，提供了对主设备和监控设备间通信序列的覆盖。 **注：**针对中断、CPU 负载等导致的执行不稳定设计相应方法。

表 D.9　传感器

安全机制/措施	见技术概览	可实现的典型诊断覆盖率	备注
通过在线监控进行失效探测	D.2.1.1	低	取决于失效探测的诊断覆盖率。
测试模式	D.2.4.1	高	—

输入比对/表决（1oo2、2oo3或者更好的冗余）	D.2.4.5	高	仅当数据流的改变出现在诊断测试间隔内。
传感器有效范围	D.2.8.1	低	探测对地或电源短路、及部分开路。
传感器相关性	D.2.8.2	高	探测有效范围内失效。
传感器合理性检查	D.2.8.3	中	—

表 D.10　执行器

安全机制/措施	见技术概览	可实现的典型诊断覆盖率	备注
通过在线监控进行失效探测	D.2.1.1	低	取决于失效探测的诊断覆盖率。
测试模式	D.2.4.1	高	—
监控（即一致性控制）	D.2.9.1	高	取决于失效探测的诊断覆盖率。

D.2 嵌入式诊断自检的技术概览

D.2.1 电气

整体目标：控制机电要素内的失效。

D.2.1.1 通过在线监控进行失效探测

注 1：表 D.2、D.3、D.5、D.9 和 D.10 引用了此技术/措施。

目的：通过监控系统对正常（在线）运行的响应行为来探测失效。

描述：在特定条件下，失效可以通过使用例如系统的时域表现信息来探测。例如，如果一个开关被正常激活，但是在预期时间内没有改变状态，则会被探测为失效。但它通常不能定位失效。

注 2：通常来说，实现在线监控不需要专门硬件要素，在线监控是探测系统在某些激活条件下的异常行为。例如，如果当车速不等于 0 时某参数翻转，那么车速与此参数之间的不匹配就会被作为失效诊断出来。

D.2.1.2 比较器

注：表 D.2 引用了此技术/措施。

目的：尽早探测出独立硬件或软件中发生的（非同时存在的）失效。

描述：比较器周期性地或连续地对独立硬件的输出信号或独立软件的输出信息进行比较，探测到的差异会生成一个失效信息。例如：两个处理单元相互交换数据（包括结果、中间结果和测试数据），每个单元中使用软件对数据进行比较，探测到的差异会生成一个失效信息。

D.2.1.3 多数表决电路

注 1：表 D.2 引用了此技术/措施。

目的：探测和屏蔽 3 个及以上通道中有 1 个发生失效的情况。

描述：表决单元使用多数原则（3 个中的 2 个，4 个中的 3 个，或者 n 个中的 m 个）来探测和屏蔽失效。

注 2：与比较器不同，即使在丢失一个通道后，多数表决技术通过确保冗余通道的功能，提高了可用性。

D.2.2 电子

整体目标：控制固态要素中的失效。

D.2.2.1 动态性原则

注：表 D.2 引用了此技术/措施。

目的：通过动态信号处理探测静态失效。

描述：对不同的静态信号（内部或外部生成）的强制改变来帮助探测要素的静态失效。该技术经常与机电要素相关。

D.2.2.2 数字信号的模拟监控

注：表 D.2 引用了此技术/措施。

目的：提升测量信号的可信性。

描述：用模拟电平来评估二进制信号，以检测非法的信号电平。

示例：某开关信号高为闭合，低为断开。对该开关的监控是检测输出电平是否在指定范围内。该指定范围的选择方式包括短路到地，短路到电源和连接器开路导致的非法电平。

D.2.3 处理单元

总体目标：探测处理单元中会导致错误结果的失效。

D.2.3.1 通过软件进行自检

注：表 D.4 引用了此技术/措施。

目标：通过软件手段尽早的探测出处理单元中和其他具有物理存储（例如，寄存器）或功能单元（例如，指令解码器或 EDC 编码/解码器）的子要素中的失效。

描述：此失效探测完全由软件实现，软件会使用一种数据模式或一套数据模式自检来测试物理存储（例如，数据和地址寄存器）或者功能单元（例如，指令解码器），或者它们两者。

示例 1：对每一个指令至少应用一个模式来测试处理单元的功能正确性。不在安全相关路径中执行的指令可以不做测试，但因未对处理单元的全部门级进行测试，所以覆盖率可能受限制。通常不可能覆盖所有的专用和特殊目的寄存器、核内定时器以及异常。对于依赖于次序的（例如流水线）或时序相关的故障模式，诊断覆盖率可能受限制。定义被测门级（而非被覆盖的指令）的实际覆盖率通常需要进行扩展的故障模拟。此测试对软错误只有非常有限的覆盖或者没有覆盖。

示例 2：对于子要素，如 EDC 编码/解码器，软件可以读取有意预写入的损坏的字来测试 EDC 逻辑的表现。如果 EDC 和存储接口有一个硬件开关来访问数据位和代码位，测试软件自身也可写入损坏的字。覆盖率取决于模式的数量和丰富程度。此测试无法覆盖软错误。

D.2.3.2 硬件支持的自检（单通道）

注：表 D.4 引用了此技术/措施。

目的：使用提高失效探测速度和扩展失效探测范围的特殊硬件，尽早探测出处理单元和其他子要素中的失效。

描述：增加的特殊硬件设施支持自检功能以便在一个门级上探测处理单元和其他子要素（例如 EDC 编码/解码器）中的失效。此测试可达到高的覆盖率。由于它的插入性本质，典型地，此测试仅在处理单元初始化或者下电时运行，并典型地用于多点故障探测。

示例：对于子要素，如 EDC 编码/解码器，可添加特殊硬件机制，如逻辑 BIST（内建自测试），以产生给编码/解码器的输入并检查是否得到期望的结果。典型地，输入可通过随机模式发生器（如 MISR）产生。它的覆盖率取决于模式的数量和丰富程度，但由于是自动模式生成，所以通常覆盖率很高。此测试无法覆盖软错误。

D.2.3.3 两个独立单元间的软件交叉自检

注：表 D.2 和 D.4 引用了此技术/措施。

目的：尽早探测出包含物理存储（例如，寄存器）和功能单元（例如，指令解码器）的处理单元中的失效。

描述：此失效探测可通过两个或更多处理单元各自执行附加软件功能自检（例如走位模式）来测试物理存储（数据和地址寄存器）和功能单元（例如，指令解码器）的方式实现。处理单元间对结果进行交换。此测试对软错误仅提供很有限的覆盖或者没有覆盖。

D.2.3.4 软件多样化冗余（单硬件通道）

注 1：表 D.4 引用了此技术/措施。

目的：通过动态软件比较法尽早探测出处理单元中的失效。

描述：设计包括在一个硬件通道中应用两个多样化的冗余软件实现方式。在某些情况下，使用不同的硬件资源（例如，不同的 RAM、ROM 存储范围）可提高诊断覆盖率。

一种实现方式，作为主路径，负责计算，如果计算错误可能导致一个危害。另一种实现方式，作为冗余路径，负责验证主路径的计算并且当探测到失效时采取相应行动。冗余路径的应用经常使用不同的算法设计和代码来提供软件多样性。当两个路径都完成计算，将对两个冗余软件应用的输出数据进行比较。探测到的差异会生成一个失效信息（见图 D.2）。此设计包含了协调两个路径和重新同步以应对瞬态错误的方法。

通常，比较会包含一些滞后和滤波，以允许由多样的软件路径产生的小差异。以算法多样性举例：A+B=C 对比 C-B=A，再比如一个通道进行常规计算而另一个通道采用二进制补码的数学运算。冗余路径可以是简单的对主路径计算结果的量值检查或变化速度限制检查。

注 2：由于主路径和冗余路径间存在潜在的共因失效，所以可采用一个额外的看门狗处理器通过问答诊断来验证主控制器的运行（见参考文献[21]）。

此安全机制的另一个版本是，通过对主路径进行原样复制（或执行两次主路径）。此版本没有软件冗余，仅能覆盖软错误。如果进行第三次代码的执行，将已知输入产生的输出和预期输出相比较，则可以达到中等覆盖率。此技术得出非常容易的合格-不合格判断准则（对比结果是否符合预期）和实现方式（无需设计冗余路径）。但是，由于多次执行同一代码，所以此概念要求保留历史项（例如，动态状态，积分电路，变化速率限制等）。

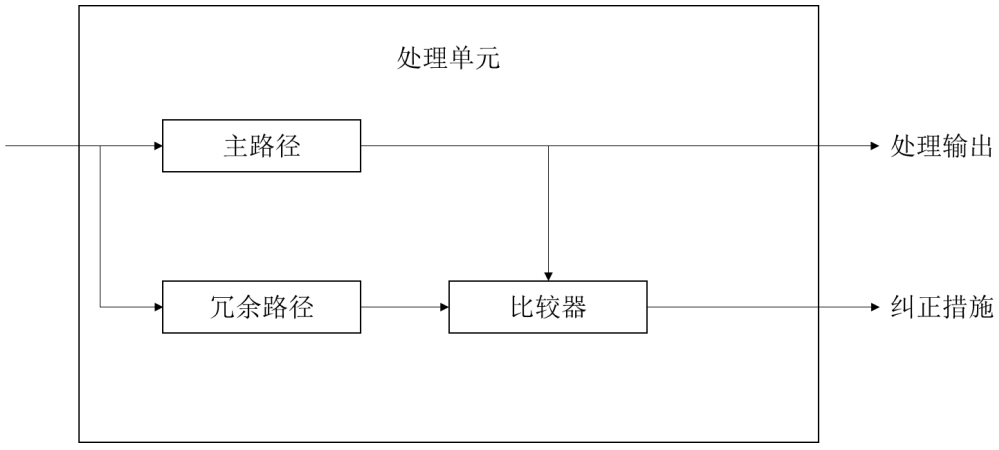


图 D.2　相同处理单元中的冗余软件比较

D.2.3.5 分立处理单元中的软件进行相互比较

注：表 D.4 引用了此技术/措施。

目的：通过软件动态比较尽早的探测出处理单元中的失效。

描述：两个处理单元相互交换数据（包括结果、中间结果和测试数据）。每个单元中的软件都会对比数据，探测出的差异会生成一个失效信息（见图 D.3）。如果采用不同的处理器类型以及分立的算法设计、代码和编译器，该方法将增加硬件和软件的多样性。此设计包含了避免因不同处理器间的差异（如回路抖动、通讯延迟、处理器初始化）而产生的假错探测的方法。

不同的路经可由双核处理器中不同的核来实现。这种情况下，此方法包括对因双核共享芯片和封装引起的共因失效模式的分析。

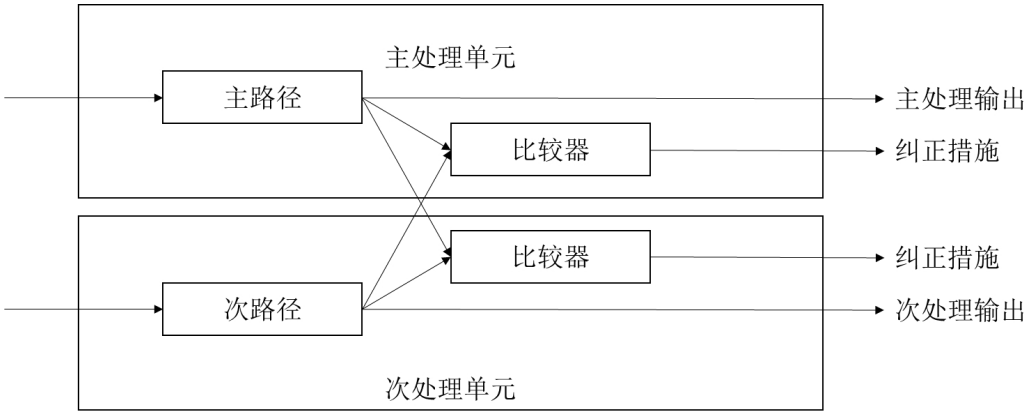


图 D.3　冗余软件比较不同处理单元

D2.3.6 硬件冗余（例如双核锁步、非对称冗余、编码处理）

注：表 D.4 引用了此技术/措施。

目的：通过逐步比较内部的或外部的结果，或比较锁步运行的两个处理单元的结果，尽早地探测出处理单元中的失效。

描述：这种诊断技术的一种形式是，一个芯片中包含双核锁步的两个对称处理单元（见参考文献[22]）。处理单元以锁步（或以固定的延迟运行）方式运行两次并将结果进行比较。任何不匹配会导致错误状态，并通常导致复位。这对于瞬态错误和 ALU 类型失效是非常有效的。基于冗余的程度，覆盖范围可扩展到存储器地址线和配置寄存器。此技术的优点在于对于并行路径不要求单独的代码，缺点是两个处理单元只提供一个处理单元的性能。在好的设计中，共因失效会被获知并被处理（例如，共同时钟失效）。此方法本身对系统性错误不能提供诊断覆盖。

其他类型的硬件冗余是可能的，例如非对称冗余。在这些架构中（如参考文献[25]），多样的专用处理单元通过一个可以逐步比较内部和外部结果的接口，与主处理单元紧密耦合。这对于直流故障模型和软错误都是非常有效的：更进一步讲，此接口降低了复杂度，缩短了错误探测等待时间，例如，影响处理单元寄存器组的故障。对于并行路径不需要单独的代码，并且专用处理单元还可以比主处理单元小。硬件的多样性提供了对共因失效和系统性失效的有效覆盖。此方法的缺点是需要一个详细的分析对诊断覆盖率进行证明。

编码处理同样是可行的：处理单元可被设计成具有特殊失效识别电路技术或者失效纠正电路技术。这些方法可保证非常小的、具有有限功能的处理器也有高覆盖率，或者适用于像 ALU 那样的子处理单元（如参考文献[26]）。硬件和软件编码可使用如安全编码处理器（见参考文献[27]）的方法进行组合。需要一个详细的分析对诊断覆盖率进行证明。

D.2.3.7 配置寄存器测试

注：表 D.4 引用了此技术/措施。

目的：尽早探测出处理单元中配置寄存器的失效。失效可以是硬件相关的（卡滞的值或软错误引发的位翻转）或软件相关的（由于软件错误导致的不正确的存储值或寄存器损坏）。

描述：读取配置寄存器的设定，然后与预期设定的编码（例如掩码）进行比较。如果设定不匹配，寄存器将会重新加载预期值。如果在预定数量的探测中错误一直存在，将会报告故障状态。

D.2.3.8 堆栈上溢出/下溢出探测

注：表 D.4 引用了此技术/措施。

目的：尽早探测出堆栈上溢出或下溢出。

描述：易失性存储器中堆栈的边界用预定值来加载。这些值被周期性地检查，如果它们发生变化，则可探测出上溢出或下溢出。如果由存储管理单元来控制对超出堆栈边界的写入，则无需进行该测试。

D.2.3.9 集成硬件的一致性监控

注：表 D.4 引用了此技术/措施。

目的：尽早探测出处理单元中的非法条件。

描述：大多数处理器具有在探测到错误时触发硬件异常处理的机制（例如除以 0 和无效的操作码）。这些错误引发的中断处理可用来捕捉这些条件以隔离系统从而免受它们的影响。典型的，硬件监控用于探测系统性失效但也可用于探测特定种类的随机硬件失效。该技术是一种好的设计实践，但对于一些代码错误的覆盖率低。

D.2.4 I/O 单元和接口

整体目标：探测输入和输出单元（数字、模拟）中的失效，并防止未经许可的输出发送给进程。

D.2.4.1 测试模式

注：表 D.5、D.9 和 D.10 引用了此技术/措施。

目的：探测静态失效（卡滞失效）和串扰。

描述：这是独立于数据流的对输入和输出单元的循环测试。用已定义的测试模式来比较观测值和相应的预期值。测试覆盖率取决于测试模式信息、测试模式接收和测试模式评估之间的独立程度。在好的设计中，测试模式不会对系统的功能性行为产生不可接受的影响。

D.2.4.2 编码保护

注：表 D.5 引用了此技术/措施。

目的：探测输入/输出数据流中的随机硬件失效和系统性失效。

描述：此方法保护输入/输出信息免受系统性失效和随机硬件失效的影响。编码保护，基于信息冗余或时间冗余或二者均冗余，提供了输入/输出单元的与数据流相关联的失效探测。典型的是把冗余信息叠加在输入、输出或两者的数据上。这提供了监控输入或输出电路正确运行的方法。许多技术都是可行的，例如，将载频信号叠加在传感器输出信号上，然后逻辑单元能检查载频的存在；或者冗余的编码位可被添加到输出通道，以允许对逻辑单元和最终执行器之间交换的信号的有效性进行监控。

D.2.4.3 多通道并行输出

注：表 D.5 引用了此技术/方法。

目的：探测随机硬件失效（卡滞失效）、外部影响导致的失效、时序失效、寻址失效、漂移失效和瞬态失效。

描述：这是一个依赖于数据流的、具有独立输出以探测随机硬件失效的多通道并行输出。失效探测通过外部比较器执行。如果发生失效，系统可能会被直接关断，此方法只有当数据流在诊断测试间隔内变化时才有效。

D.2.4.4 受监控的输出

注：表 D.5 引用了此技术/方法。

目的：用于探测独立失效、由外部影响导致的失效、时序失效、寻址失效、漂移失效（对于模拟信号）和瞬态失效。

描述：这是一个依赖于数据流的独立输入和输出的比较，以确保符合预先定义的公差范围（时间、值）。探测到的失效不会一直与缺陷的输出相关联，此方法只有当数据流在诊断测试间隔内变化时才有效。

D.2.4.5 输入比较/表决

注：表 D.5 和表 D.9 引用了此技术/方法。

目的：用于探测独立失效、由外部影响导致的失效、时序失效、寻址失效、漂移失效（对于模拟信号）和瞬态失效。

描述：这是一个依赖于数据流的独立输入比较，以确保符合已定义的公差范围（时间、值）。可以是 2 取 1、3 取 2 或更好的冗余。此方法只有当数据流在诊断测试间隔内变化时才有效。

D.2.5 通信总线

整体目标：探测信息传递的失效。

D.2.5.1 一位硬件冗余

注：表 D.6 引用了此技术/方法。

目的：用于探测每一个奇数位失效，即探测数据流中所有可能的位失效的 50%。

描述：通信总线扩展了一条线（位），这条增加的线（位）通过奇偶校验来探测失效。

示例：标准 UART（通用异步收发传输器）中实施的奇偶校验位。

D.2.5.2 多位硬件冗余

注：表 D.6 引用了此技术/方法。

目的：用于探测总线通讯和串行传输链通讯中的失效。

描述：通信总线扩展两条或更多条线，利用这些增加的线并通过块编码技术来探测失效（例如，汉明码、里德所罗门码、CRC、低密度奇偶校验码等）。

D.2.5.3 完整硬件冗余

注：表 D.6 引用了此技术/方法。

目的：通过对比两条总线上的信号来探测通信中的失效。

描述：总线被复制，额外的总线用于探测失效。

示例：双通道 FlexRay 应用：总线被复制，额外的线（位）用于探测失效。

D.2.5.4 使用测试模式检验

注：表 D.6 引用了此技术/方法。

目的：用于探测静态失效（卡滞失效）和串扰。

描述：这是不依赖于数据流的数据路径循环测试，使用一个已定义的测试模式来比较观测值和相应的预期值。

测试覆盖率依赖于测试模式信息、测试模式接收、测试模式评估之间的独立程度，在好的设计中，测试模式不会对系统的功能性行为产生不可接受的影响。

D.2.5.5 发送冗余

注：表 D.6 引用了此技术/方法。

目的：探测总线通信中的瞬态失效。

描述：信息被依次发送几次，此技术只对探测瞬态失效有效。

D.2.5.6 信息冗余

注 1：表 D.6 引用了此技术/方法。

目的：探测总线通信中的失效。

描述：数据按块传输，每块均含一个计算的“检验和”或“CRC”（循环冗余码校验）（参考目录[28]和[29]），接收方随后根据接收到的数据重新计算校验和，并与收到的校验和做比较。CRC 的覆盖率依

赖于被覆盖的数据的长度、CRC 的大小（位数）和多项式。CRC 可被设计为用于处理更多可能的底层硬件通信失效模式（比如突发错误）。

信息 ID 可能包含在校验和/CRC 计算中，以提供对此部分信息的损坏覆盖（信息伪装）。

a) 数据传输中失效模式的总体覆盖率较低：汉明距离是 2 或更少

示例 1：CRC 的值嵌入在信息中；对数据长度小于 2048 位的数据，5 位的 CRC 和多项式 0x12 的汉明距离是 2。发送方包含上述 CRC 值，接收方在通过计算并比较 CRC 值后确认数据。

b) 数据传输中失效模式的总体覆盖率中等：汉明距离是 3 或更多

示例 2：CRC 值嵌入在信息中；对长度小于 119 位的数据，8 位 CRC 和多项式 0x97 的汉明距离是 4。发送方包含上述 CRC 值，接收方在通过计算并比较 CRC 值后确认数据（典型应用在 LIN 总线中）。

示例 3：CRC 值嵌入在信息中；对长度小于 501 位的数据，10 位的 CRC 和多项式 0x319 的汉明距离是 4。发送方包含上述 CRC 值，接收方在通过计算并比较 CRC 值后确认数据。

示例 4：CRC 值嵌入在信息中；对长度小于 127 位的数据，15 位的 CRC 和多项式 0x4599 的汉明距离是 5。同样的，长度最大为 15 位的突发错误能够被探测出来。发送方包含上述 CRC 值，接收方在通过计算并比较 CRC 值后确认数据（应用在 CAN 总线中）。

示例 5：CRC 值嵌入在信息中；对长度小于或等于 248 字节的数据，24 位 CRC 和多项式 0x5D6DCB 的汉明距离是 6；对长度大于 248 字节的数据，CRC 的汉明距离是 4。发送方包含上述 CRC 值，接收方通过计算并比较 CRC 值后确认数据（如在 FlexRay 中消息帧 CRC 的使用）。

示例 6：信息报头（包括 ID）的 CRC 值嵌入在该信息中；对长度小于或等于 20 位的数据，11 位 CRC 和多项式 0x385 的汉明距离是 6。发送方包含上述 CRC 值，接收方通过计算并比较 CRC 值后确认数据（如在 FlexRay 中消息报头 CRC 的使用）。

注 2：对数据和 ID 的损坏的探测可以达到高覆盖率，然而，仅通过一个特征码检查数据和 ID 的一致性是达不到整体高覆盖率的，无论特征码的作用有多大。特别地，特征码不能覆盖信息丢失或者非期望的信息重复。

注 3：如果检验和算法的汉明距离小于 3，若有适当的理由，仍能声明对数据和 ID 损坏达到高覆盖率。

D.2.5.7 帧计数器

注：表 D.6 引用了此技术/方法。

目的：用于探测帧丢失。帧是控制器发送给另一控制器的一系列连贯的数据。通过信息的 ID 来识别唯一的帧。

描述：总线上传输的每个单独的安全相关帧包含一个作为信息一部分的计数器。在生成每个连续帧时计数器值增加（翻转）。接收方随后能通过验证计数器的值是否增加了 1 来探测任何的帧丢失或者帧未更新。

一个特殊版本的帧计数器将包含单独的信号计数器，这些计数器同安全相关数据的更新相关联。在此情况下，如果一个帧包含超过一条安全相关的数据，那么将为每条安全相关数据提供一个独立的计数器。

D.2.5.8 超时监控

注：表 D.6 引用了此技术/方法。

目的：探测发送和接收节点间的数据丢失。

描述：接收方监控每个预期的安全相关信息 ID，对接收到的具有该信息 ID 的有效帧之间的时间进行监控。两条信息间过长的时间间隔会被识别为失效。这旨在探测信道的持续丢失或一个特定信息的连续丢失（未收到特定信息 ID 的帧）。

D.2.5.9 发送信息回读

注 1：表 D.6 引用了此技术/方法。

目的：探测总线通信失效。

描述：发送方从总线上回读已发送信息并与原始信息做比较。

注 2：此安全机制在 CAN 上使用。

注3：对于数据和ID的损坏可以达到高覆盖率，然而，仅通过检查数据和ID的一致性是达不到整体高覆盖率的。其他的失效模式，如非预期的消息重复，是不一定被此安全机制覆盖到的。

D.2.6 电源

整体目标：探测电源缺陷导致的失效。

D.2.6.1 电压或电流控制（输入）

注：表D.7引用了此技术/方法。

目的：尽快探测错误的输入电流或电压值。

描述：监控输入电压或电流。

D.2.6.2 电压或电流控制（输出）

注：表D.7引用了此技术/方法。

目的：尽快探测错误的输出电流或电压值。

描述：监控输出电压或电流。

D.2.7 程序序列的时间和逻辑监控

注：表D.8引用了这组技术/方法。

整体目标：用于探测有缺陷的程序序列。如果程序的单个要素（比如，软件模块、子程序或指令）运行在错误的时序或时段，或处理器时钟有故障的时候，则存在一个缺陷的程序序列。

D.2.7.1 具有独立时间基准，无时间窗口的看门狗

注：表D.8引用了此技术/方法。

目的：监控程序序列的表现和合理性。

描述：具有独立时间基准的外部时序要素（例如，看门狗定时器）被周期性触发，以监控处理器的行为和程序序列的合理性。触发点被正确放置在程序中是非常重要的。不以固定周期触发看门狗，但定义了一个最大的时间间隔。

D.2.7.2 具有独立时间基准，有时间窗口的看门狗

注：表D.8引用了此技术/方法。

目的：监控程序序列的表现和合理性。

描述：具有独立时间基准的外部时序要素（例如，看门狗定时器）被周期性触发，以监控处理器的行为和程序序列的合理性。触发点被正确放置在程序中是非常重要的（如，不在中断服务程序中）。为看门狗定时器设定上限和下限。如果程序序列耗费了比期望时间更长或更短的时间，将采取措施。

D.2.7.3 程序序列的逻辑性监控

注：表D.8引用了此技术/方法。

目的：监控单个程序段的正确次序。

描述：用软件（计数程序、关键程序）或用外部监控设备（参考[23,24]）来监控各程序段的正确次序。非常重要的是，检查点要被放置在程序中，用来监控由于单点或多点故障导致的程序未能执行完成或执行程序错乱的危险路径。次序可在各函数调用间被更新或更紧密的集成于程序执行中。

D.2.7.4 程序序列的时间和逻辑的联合监控

注：表D.8引用了此技术/方法。

目的：监控单个程序段的行为和正确次序。

描述：监控程序序列的时间设备（例如看门狗定时器）只有当程序段的次序被正确执行时才会被触发。此方法是D.2.7.3与D.2.7.1（或D.2.7.2）的技术组合。

D.2.7.5 基于时间的程序序列的时间和逻辑联合监控

注：表 D.8 引用了此技术/方法。

目的：监控单个程序段的行为、正确的次序和执行的时间间隔。

描述：在一个相关时间窗口内，于期望发生软件更新点处应用程序流监控策略。程序流监控的时序结果和时间的计算由外部监控设备监控。

D.2.8 传感器

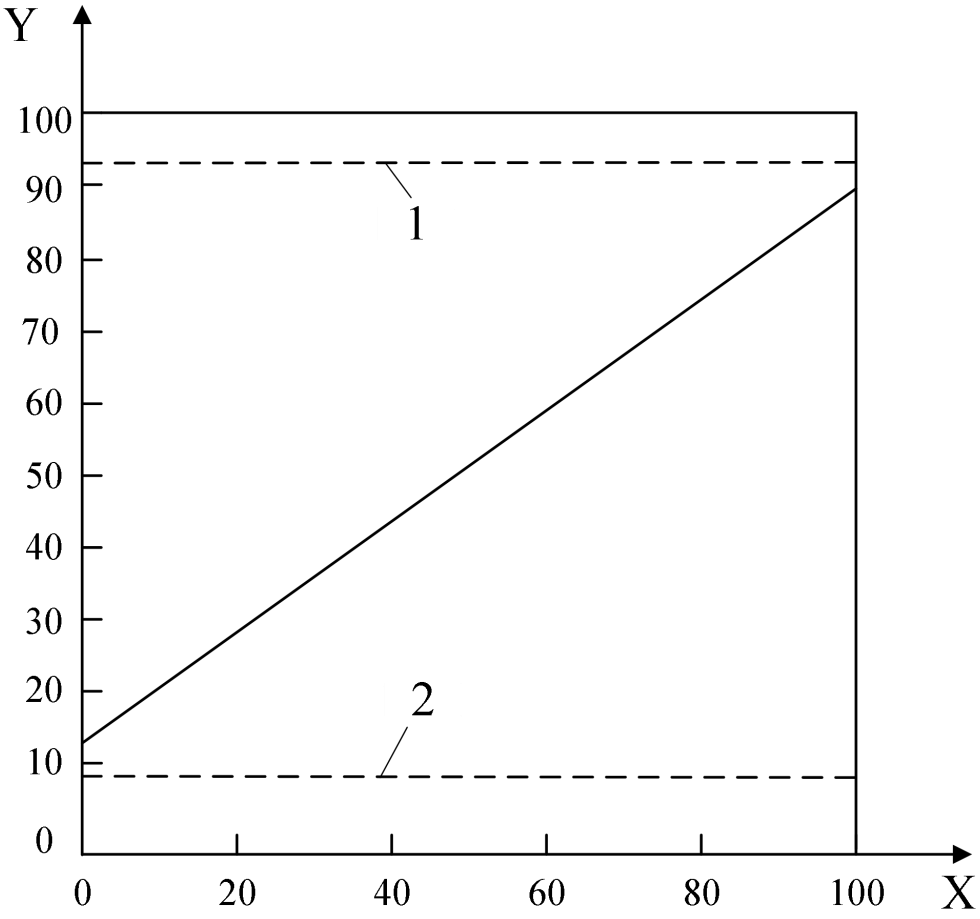
整体目标：控制系统的传感器失效。

D.2.8.1 传感器的有效范围

注：表 D.9 引用了此技术/方法。

目的：探测传感器短路到地或电源，及一些断路。

描述：将有效读数限制在传感器电气范围的中间部分（例如，见图 D.4），如果传感器读取在无效区域，则表明传感器发生了电气问题，如短路到电源或地。ECU 一般使用 ADC 读取传感器值。



说明：

X ——传感器物理读数，以%表示

Y ——传感器测量读数，以参考电压的%表示

1 ——超量程的高门限

2 ——超量程的低门限

图 D.4　带有超量程区域的传感器

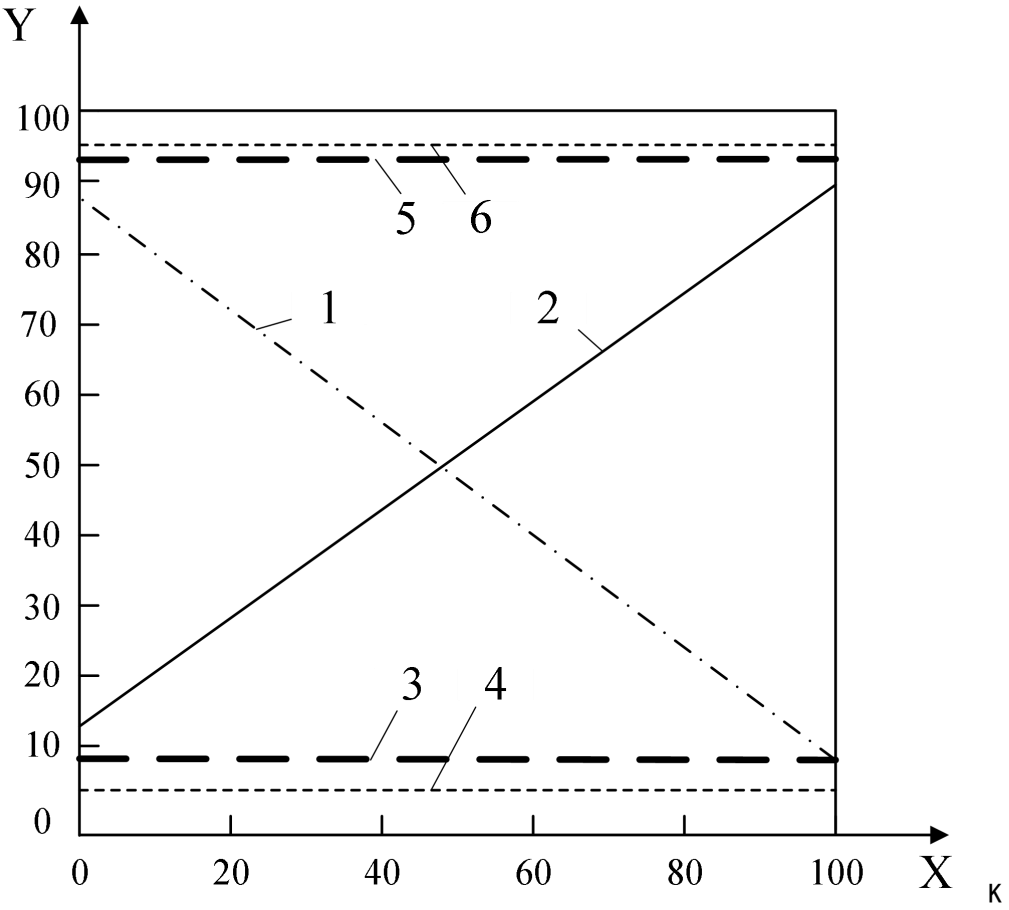
D.2.8.2 传感器相关性

注：表 D.9 引用了此技术/方法。

目的：使用冗余传感器探测传感器量程内的漂移、偏移或其他错误。

描述：通过比较两个一样或者相似的传感器，来探测量程内的失效，比如漂移、偏移或卡滞失效。例如，见图 D.5，两个斜率相同但方向相反的传感器。应指出的是，每个传感器超量程的区域是不同的。ECU 一般通过 ADC 读取传感器值。

如图 D.5 的例子，传感器将被转换成相等斜率，并在一个阈值范围内比较。选定阈值时需考虑 ADC 公差范围和电气要素的变差。ECU 在采样两个传感器的值时需要尽可能的同步以避免因传感器读数的动态变化导致错误的失效探测。



说明：

X ——传感器物理读数，以%表示

Y ——传感器测量读数，以参考电压的%表示

1 ——传感器 1

2 ——传感器 2

3 ——传感器 1 的超量程低门限

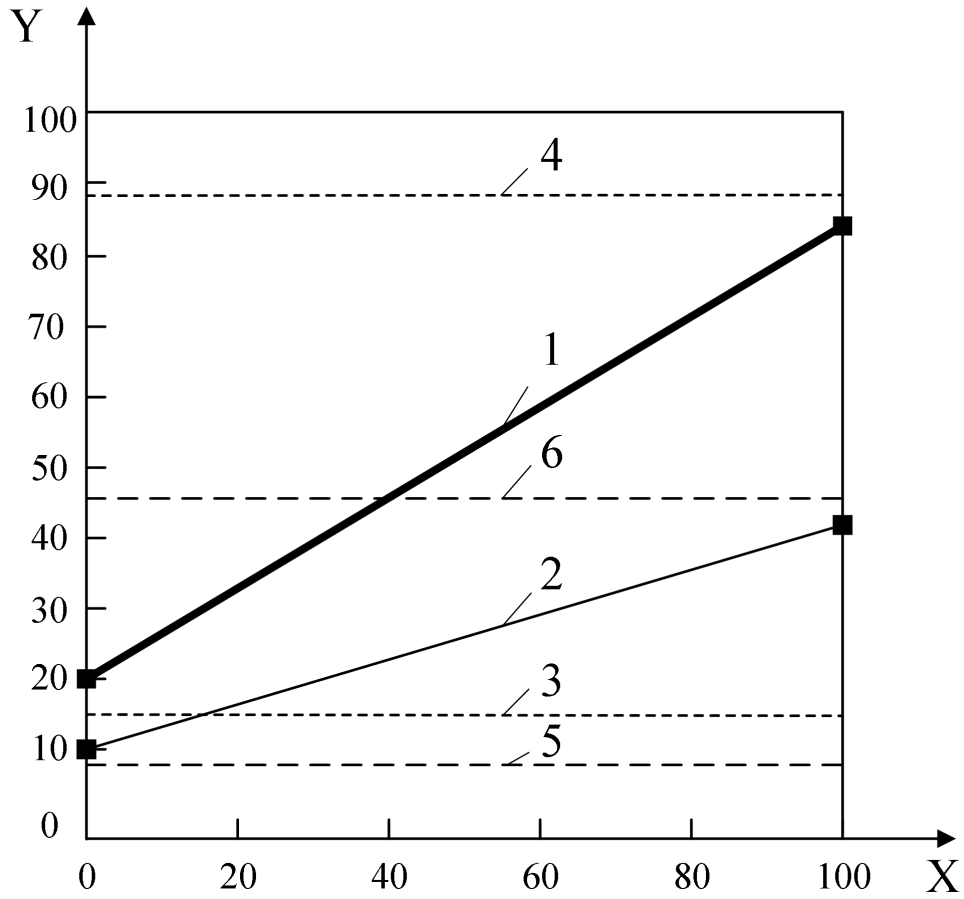
4 ——传感器 2 的超量程低门限

5 ——传感器 1 的超量程高门限

6 ——传感器 2 的超量程高门限

图 D.5　斜率相等但方向相反的并带有超量程区域的传感器

基于相等斜率传感器的诊断，不能探测以下情况：当两个传感器短路在一起并在交叉点上产生相关读数时；或由于单个组件（如 ADC）导致的共因失效，会以相似的方式破坏两个传感器的结果。一个替代方案是如图 D.6 中的一个传感器斜率是另一个的一半的设计。



说明：

X ——传感器物理读数，以%表示

Y ——传感器测量读数，以参考电压的%表示

1 ——传感器 1

2 ——传感器 2

3 ——传感器 1 的超量程低门限

4 ——传感器 2 的超量程低门限

5 ——传感器 1 的超量程高门限

6 ——传感器 2 的超量程高门限

图 D.6　一个斜率是另一个一半的并带有超量程区域的传感器

D.2.8.3 传感器合理性检查

注：表 D.9 引用了此技术/方法。

目的：使用多个不同的传感器来探测传感器量程内的漂移、偏移或其他错误。

描述：比较测量不同参数的两个（或更多）传感器，以探测量程内的失效，比如漂移、偏移或其卡滞失效。使用模型将传感器的测量值转换成等效值以进行比较。

示例：比较汽油发动机节气门位置、进气歧管压力及空气流量传感器，每一个都转换成空气流量值后进行比较，使用多种传感器的用法可降低系统性故障的问题。

D.2.9 执行器

整体目标：控制系统执行端要素的失效。

D.2.9.1 监控

注 1：表 D.10 引用了此技术/方法。

目的：探测执行器的不正确运行。

描述：监控执行器的运行。

注 2：可在执行器层面通过物理参数的测量（有高覆盖率）来进行监控，也可在系统层面对执行器的失效影响进行监控。

示例 1：对冷却风扇，使用温度传感器在系统层面对其进行监控以探测失效。物理参数的监测可测量冷却风扇的输入电压、电流或两者。

示例 2：用反馈控制将节气门阀叶片移动到期望位置。测量出节气门实际位置并与期望位置做比较，期望位置是由节气门位置指令和期望的性能模型所决定的。如果在考虑迟滞因素后，两个值仍不同，则可以报错。

附 录 E

（资料性）

硬件架构度量示例计算：“单点故障度量”和“潜伏故障度量”

本附录给出了一个示例，该示例根据 8.4.7 和 8.4.8 的选项 a）的要求，对相关项的每一个安全目标计算单点故障度量和潜伏故障度量。

本示例中的系统（见图 E.1）在一个 ECU 中实现了两个功能。

功能 1 有一个输入（通过传感器 R3 测量的温度）和一个输出（通过 I71 控制的阀 2），其功能是当温度高于 90℃时打开阀 2。

如果没有电流经过 I71，阀 2 打开。

相关联的安全目标 1 是“当温度高于 100 ℃时关闭阀 2 的时间不得长于 100 ms”。安全目标被分配为 ASIL B 等级。安全状态是：阀 2 打开。

微控制器的ADC读取传感器 R3 的值。R3 的电阻值随着温度升高而降低。该输入没有监控。控制 T71 的输出级由模拟输入 InADC1（表中的安全机制 SM1）来监控。在这个例子中，我们假设，安全机制 SM1 能够对 T71 有可能违背安全目标的失效模式进行探测，且具备 90%的诊断覆盖率。如果 SM1 探测到失效，安全状态被激活但是没有点灯。因此，声明针对 SM1 探测失效模式的潜伏故障的诊断覆盖率仅为 80%（驾驶员将通过功能降级获悉失效）。

功能 2 有两个输入（通过传感器 I1 和 I2 生成脉冲来测量轮速）和一个输出（通过 I61 控制阀 1），其功能是当车速高于 90km/h 时打开阀 1。

如果没有电流经过 I61，阀 1 打开。

相关联的安全目标 2 是“当速度超过 100km/h 时关闭阀 1 的时间不得长于 200 ms”。安全目标被分配为 ASIL C 等级。安全状态为：阀 1 打开。

微控制器读取 I1 和 I2 的脉冲值。通过这些传感器给出的平均值计算轮速。安全机制 2 （表中的安全机制 SM2）比较两个输入。SM2 对每个输入的失效探测达到 99%的诊断覆盖率。如果出现不一致，输出 1 设为 0。 阀 1 打开（晶体管电压为“0”则打开栅极。I61 电压为“0”则打开阀 1）。因此，99%可能导致违背安全目标的故障能被探测到并且进入安全状态。当安全状态被激活时，灯 L1 点亮。因此，这些故障是 100%能被察觉的。剩下的 1%的故障是残余故障而不是潜伏故障。

控制 T61 的输出级被模拟量输入 In ADC2（表中的安全机制 SM3）监控。

微控制器没有内部冗余。在此示例中，假定安全故障的比例为 50%。并假定通过内部自检和外部看门狗（表中的安全机制 SM4）达到对违背安全目标的总体覆盖率为 90%。看门狗通过微控制器的输出 0 得到喂狗信号。当看门狗不再被刷新，其输出变低。SM4（看门狗和微控制器自检）提供的故障探测把这两个功能切换到它们的安全状态并点亮 L1。因此，针对潜伏故障的诊断覆盖率声称是 100%。

L1 是仪表板上的一个 LED 灯，当探测到多点失效（其中只有一部分可以被探测到）时点亮它，并提示驾驶员功能 2（打开阀 1）的安全状态已被激活。

注 1：在该示例中不考虑线束失效。

注 2：用于一个给定电子元器件的故障模型可以根据应用而不同。

示例 1：电阻的故障模型取决于硬件元器件是被用于数字输入（例如 R11、R12、R13 等）还是模拟输入（例如 R3）。 在第一种情况下故障模型可以是“开路/短路”，而在第二种情况下它可以是“开路/短路/漂移”。

注 3：第一个度量仅使用了目的是防止违背安全目标的安全机制的失效模式覆盖率。 第二个度量仅使用了目的在于防止失效模式变成潜伏的安全机制的失效模式覆盖率。

示例 2：R21 的失效模式“开路”在缺乏安全机制时有违背安全目标 2 的可能性。安全机制 2 以 99%的失效模式覆盖率探测这种失效模式，并将系统切换到安全状态。当探测到这种失效模式，显示一个警告；针对潜伏失效的失效模式覆盖率是 100%。

注 4：在本示例中，已考虑关于硬件要素失效模式分布的假设。如果没有表明或引用特定的失效模式分布，可以假设失效模式平均分布。

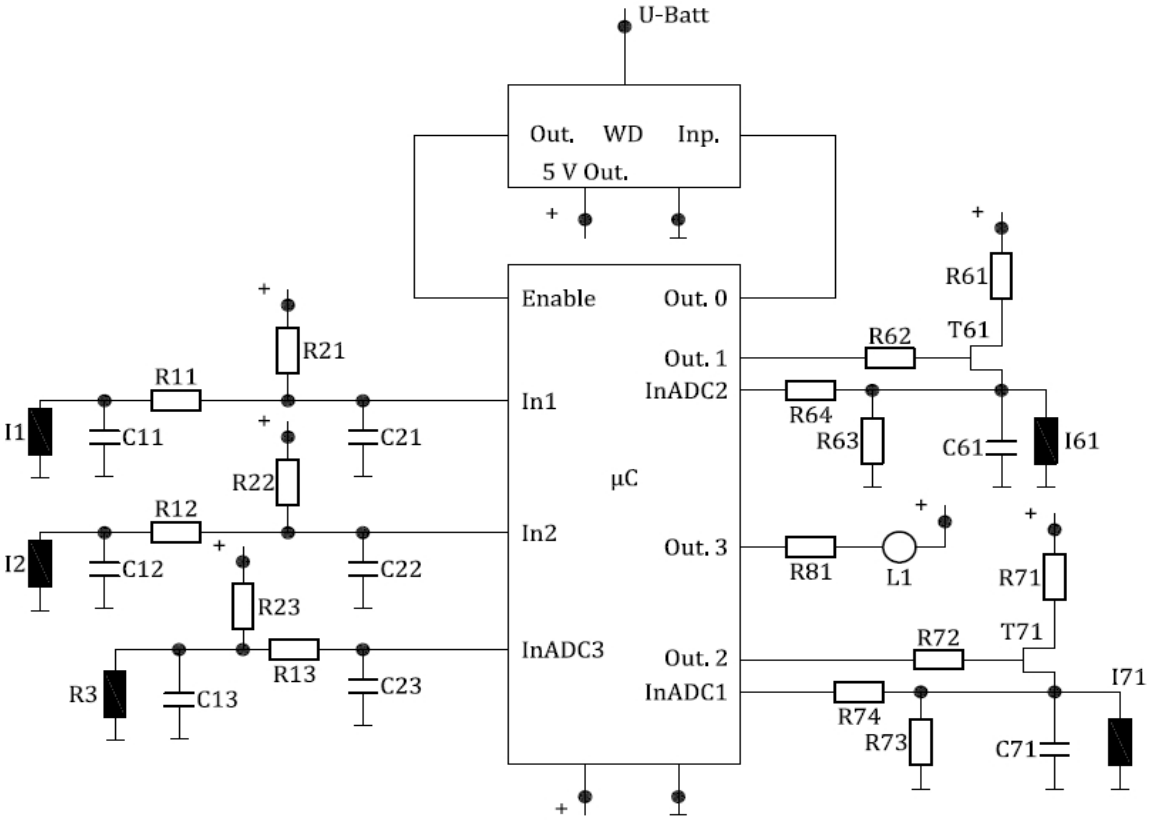


图 E.1　示例图

表 E.1　安全目标 1

组件名	失效率/FIT	在计算中是否考虑安全相关组件？	失效模式	失效模式分布	在缺少安全机制时失效模式是否有可能违背安全目标？	是否有防止失效模式违背安全目标的安全机制？	考虑到违背安全目标的失效模式覆盖率	残余或单点故障失效率/FIT	在结合其他组件的无关失效时失效模式是否会违背安全目标？	探测方法？是否有防止失效模式成为潜伏的安全机制？	考虑到潜伏失效的失效模式覆盖率	潜伏多点故障失效率/FIT
R3 注 1	3	是	开路	30%	X	无	0%	0.9				
			短路	10%								
			漂移 0.5	30%								
			漂移 2	30%	X		0%	0.9				
R13 注 1，注 2 和注 6	2	是	开路	90%	X	无	0%	1.8				
			短路	10%	X		0%	0.2				
R23 注 1	2	是	开路	90%		无						
			短路	10%	X		0%	0.2				

组件名	失效率/FIT	在计算中是否考虑安全相关组件？	失效模式	失效模式分布	在缺少安全机制时失效模式是否有可能违背安全目标？	是否有防止失效模式违背安全目标的安全机制？	考虑到违背安全目标的失效模式覆盖率	残余或单点故障失效率/FIT	在结合其他组件的无关失效时失效模式是否会违背安全目标？	探测方法？是否有防止失效模式成为潜伏的安全机制？	考虑到潜伏失效的失效模式覆盖率	潜伏多点故障失效率/FIT
C13 注 3 和注 6	2	是	开路	20%	X	无	0%	0.4				
			短路	80%								
C23 注 4	2	否	开路	20%								
			短路	80%								
WD	20	是	输出卡滞在 1	50%					X	无	0%	10
			输出卡滞在 0	50%								
T71 注 5	5	是	开路	50%		SM1				SM1		
			短路	50%	X		90%	0.25	X		80%	0.45
R71 注 2 和注 6	2	是	开路	90%						无		
			短路	10%					X		0%	0.2
R72 注 2 和注 6	2	是	开路	90%						无		
			短路	10%					X		0%	0.2
R73 注 4	2	否	开路	90%								
			短路	10%								
R74 注 2 和注 6	2	是	开路	90%					X	无	0%	1.8
			短路	10%					X		0%	0.2
171 注 4	5	否	开路	80%								
			短路	20%								
C71 注 3	2	是	开路	20%					X	无		0.4
			短路	80%								
R81 注 4	2	否	开路	90%								
			短路	10%								
L1	10	否	开路	90%								

组件名	失效率/FIT	在计算中是否考虑安全相关组件？	失效模式	失效模式分布	在缺少安全机制时失效模式是否有可能违背安全目标？	是否有防止失效模式违背安全目标的安全机制？	考虑到违背安全目标的失效模式覆盖率	残余或单点故障失效率/FIT	在结合其他组件的无关失效时失效模式是否会违背安全目标？	探测方法？是否有防止失效模式成为潜伏的安全机制？	考虑到潜伏失效的失效模式覆盖率	潜伏多点故障失效率/FIT
注 4			短路	10%								
μC	100	是	全部	50%	X	SM4	90%	5	X	SM4	100%	0
			全部	50%								
							Σ 9.65				Σ 13.25	

总失效率 163 FIT

单点故障度量 = 1-(9.65/142) = 93.2%

潜伏故障度量 =1-(13.25/(142-9.65)) =90.0%

总安全相关 142 FIT

总非安全相关 21 FIT

安全目标 1 被分配为 ASIL B 等级，对于 ASIL B 等级，如果采用表 4，单点故障度量推荐为≥90%，以及，如果采用表 5，潜伏故障度量推荐为≥60%。单点故障度量的计算值为 93.2%表明此度量已被满足，同时潜伏故障度量的计算值为 90%表明潜伏故障度量也被满足（见表 E.1）。

注 1：R3 和 R13 的失效模式“开路”和 R23 的失效模式“短路”是单点故障。它们直接导致违背安全目标并且没有安全机制覆盖这些硬件元器件的故障。

注 2：此硬件元器件的目的是提供电气保护。失效模式“短路”意味着失去保护。

注 3：此硬件元器件的目的是提供 ESD 保护。失效模式“开路”意味着失去保护。

注 4：计算中为了保守起见，不用考虑对违背安全目标没有显著贡献可能性的失效要素，也就是不用考虑仅有安全失效模式的要素。这里，L1 和 R81 是实施了防止双点故障成为潜伏故障的安全机制的要素。n 阶（n>2）的多点故障被认为是安全故障。

注 5：直接导致违背安全目标的故障（单点故障或残余故障）不会再提高潜伏故障的总数。因此，例如，T71 的潜伏失效模式“栅极短路”的失效率按下述公式计算：

$$\lambda_{MPF,L} = [(\lambda_{T71} \times D_{FM,closed\ gate}) - \lambda_{T71,RF}] \times (1 - F_{MC,latent\ faults})$$

$$\lambda_{MPF,L} = [(5 \times 0.5) - 0.25] \times (1 - 0.8) = 0.45$$

注 6：导致失去 ESD 或电气保护的失效模式的归类是基于个案分析，并考虑 ESD 或电应力的可能性及关于安全目标的 ESD 或电应力特征效应。如果，例如 ESD 事件可能在车辆全生命周期内发生，且它的后果可导致在缺少给定保护条件下违背安全目标，那么导致失去保护的失效模式被归类为单点故障。本附录就是关于如何在度量内处理那些情况的示例。在实践中，ESD 或 EMI 应力对典型设计的影响与示例不同。

表 E.2 安全目标 2

组件名	失效率/FIT	在计算中是否考虑安全相关组件?	失效模式	失效模式分布	在缺少安全机制时失效模式是否有可能违背安全目标?	是否有防止失效模式违背安全目标的安全机制?	考虑到违背安全目标的失效模式覆盖率	残余或单点故障失效率/FIT	在结合其他组件的无关失效时失效模式是否会违背安全目标?	探测方法?是否有防止失效模式成为潜伏的安全机制?	考虑到潜伏失效的失效模式覆盖率	潜伏多点故障失效率/FIT
R11 注 1,注 6 和注 7	2	是	开路	90 %	X	SM2	99 %	0.018	X	SM2	100 %	0
			短路	10 %	X		99 %	0.002	X		100 %	0
R12 注 1,注 6 和注 7	2	是	开路	90 %	X	SM2	99 %	0.018	X	SM2	100 %	0
			短路	10 %	X		99 %	0.002	X		100 %	0
R21 注 2	2	是	开路	90 %	X	SM2	99 %	0.018	X	SM2	100 %	0
			短路	10 %	X		99 %	0.002	X		100 %	0
R22 注 2	2	是	开路	90 %	X	SM2	99 %	0.018	X	SM2	100 %	0
			短路	10 %	X		99 %	0.002	X		100 %	0
C11 注 1,注 6 和注 7	2	是	开路	20 %	X	SM2	99 %	0.004	X	SM2	100 %	0
			短路	80 %	X		99 %	0.016	X		100 %	0
C12 注 1,注 6 和注 7	2	是	开路	20 %	X	SM2	99 %	0.004	X	SM2	100 %	0
			短路	80 %	X		99 %	0.016	X		100 %	0
C21	2	是	开路	20 %		SM2				SM2		
			短路	80 %	X		99 %	0.016	X		100 %	0
C22	2	是	开路	20 %		SM2				SM2		
			短路	80 %	X		99 %	0.016	X		100 %	0
I1	4	是	开路	70 %	X	SM2	99 %	0.028	X	SM2	100 %	0
			短路	20 %	X		99 %	0.008	X		100 %	0
			漂移 0.5	5 %	X		99 %	0.002	X		100 %	0
			漂移 2	5 %								
I2	4	是	开路	70 %	X	SM2	99 %	0.028	X	SM2	100 %	0
			短路	20 %	X		99 %	0.008	X		100 %	0
			漂移 0.5	5 %	X		99 %	0.002	X		100 %	0

组件名	失效率/FIT	在计算中是否考虑安全相关组件?	失效模式	失效模式分布	在缺少安全机制时失效模式是否有可能违背安全目标?	是否有防止失效模式违背安全目标的安全机制?	考虑到违背安全目标的失效模式覆盖率	残余或单点故障失效率/FIT	在结合其他组件的无关失效时失效模式是否会违背安全目标?	探测方法?是否有防止失效模式成为潜伏的安全机制?	考虑到潜伏失效的失效模式覆盖率	潜伏多点故障失效率/FIT
			漂移 2	5 %								
WD	20	是	输出卡滞在 1	50 %					X	无	0 %	10
			输出卡滞在 0	50 %								
T61	5	是	开路	50 %		SM3				SM3		
			短路	50 %	X		90 %	0.25	X		100 %	0
R61 注 3 和注 6	2	是	开路	90 %						无		
			短路	10 %					X		0 %	0.2
R62 注 3 和注 6	2	是	开路	90 %						无		
			短路	10 %					X		0 %	0.2
R63 注 5	2	否	开路	90 %								
			短路	10 %								
R64 注 1 和注 6	2	是	开路	90%					X	无	0%	1.8
			短路	10%					X		0%	0.2
I61 注 5	5	否	开路	80%								
			短路	20%								
C61 注 4 和注 6	2	是	开路	20%					X	无	0%	0,4
			短路	80%								
R81 注 5	2	否	开路	90%								
			短路	10%								
L1 注 5	10	否	开路	90%								
			短路	10%								
μC	100	是	全部	50%	X	SM4	90%	5	X	SM4	100%	0

组件名	失效率/FIT	在计算中是否考虑安全相关组件？	失效模式	失效模式分布	在缺少安全机制时失效模式是否有可能违背安全目标？	是否有防止失效模式违背安全目标的安全机制？	考虑到违背安全目标的失效模式覆盖率	残余或单点故障失效率/FIT	在结合其他组件的无关失效时失效模式是否会违背安全目标？	探测方法？是否有防止失效模式成为潜伏的安全机制？	考虑到潜伏失效的失效模式覆盖率	潜伏多点故障失效率/FIT
			全部	50%								
							Σ 5.48				Σ 12.80	

总失效率 176 FIT

总安全相关 157 FIT

总非安全相关 19 FIT

单点故障度量 = 1-（5.48/157）=96.5%

潜伏故障度量 = 1-（13.99（157-5.48））=91.6%

安全目标 2 被分配为 ASIL C 等级，其中，如果采用表 4，单点故障度量要求≥97%；如果采用表 5，潜伏故障度量建议≥80%。单点故障度量的计算值为 96.5%表明此度量要求未被满足，同时潜伏故障度量的计算值为 91.6%，表明潜伏故障度量得到满足（见表 E.2）。

注 1：此硬件元器件的目的是电气保护。失效模式之一是失去电气保护。其他模式是在缺乏安全机制时有违背安全目标的可能性。

注 2：在两种情况下，两种失效模式都有在缺乏安全机制时违背安全目标的可能性，无法发送速度脉冲。这导致错误的速度采集。该传感器是一个集电极开路传感器。

注 3：此硬件元器件的目的是提供电气保护。失效模式“短路”意味着失去保护。

注 4：此硬件元器件的目的是提供 ESD 保护。失效模式“开路”意味着失去保护。

注 5：计算中为了保守起见，不用考虑对违背安全目标没有显著贡献可能性的失效要素，也就是不用考虑仅有安全失效模式的要素。例如，此处的 L1 和 R81 是实施了防止双点故障成为潜伏故障的安全机制的要素。n>2 的多点故障被认为是安全故障。

注 6：导致失去 ESD 或电气保护的失效模式的归类是基于个案分析，并考虑 ESD 或电应力的可能性及关于安全目标的 ESD 或电应力特征效应。如果，例如 ESD 事件可能在车辆全生命周期内发生，且它的后果可导致在缺少给定保护条件下违背安全目标，那么导致失去保护的失效模式被归类为单点故障。本附录就是关于如何在度量内处理那些情况的示例。在实践中，ESD 或 EMI 应力对典型设计的影响与示例不同。此外，这里也考虑到 SM4 没有覆盖这些失效模式，即使它们可以导致微控制器的某些损坏。

注 7：失去电气保护将导致错误的输入值，并且将被 SM2 探测到，因此不会变成潜伏。

附 录 F

（资料性）

按照 4.2 的要求满足第九章目标的论据示例

F.1 总则

本附录给出了如何基于安全分析的结果来评估硬件设计是否满足第 9 章目标的示例。本示例是基于附录 E 对安全目标 2（当速度超过 100km/h 时阀 1 的关闭时间不得长于 200ms [ASIL C 等级]）的硬件设计和分析。评估过程按照下述步骤执行：

a) 通过安全分析评估 PMHF；

b) 定义评估故障或失效模式的选择标准；

c) 应用选择标准；

d) 评估第 9 章目标的符合性。

F.2 通过安全分析评估 PMHF

评估的起点是附录 E 中已经完成的功能安全分析。除了附录 E 的评估外，还要使用下述公式估算 PMHF 值：PMHFest = λSPF + λRF+ λDPF_det × λDPF_latent × TLifetime（有关更详细的如何估算 PMHF 值的信息，见 GB/T 34590.10-XXXX 中关于 PMHF 计算的相关章节），同时计算每个失效模式对总 PMHF 值贡献的百分比。

表 F.1 附录 E 安全目标 2 的定量 FMEA

组件名	失效率/FIT	在计算中是否考虑安全相关组件?	失效模式	失效模式分布	在缺少安全机制时失效模式是否有可能违背安全目标?	是否有防止失效模式违背安全目标的安全机制?	考虑到违背安全目标的失效模式覆盖率	残余或单点故障失效率/FIT	在结合其他组件的无关失效时失效模式是否会违背安全目标?	探测方法? 是否有防止失效模式成为潜伏的安全机制?	考虑到潜伏失效的失效模式覆盖率	潜伏多点故障失效率/FIT	DPF_det	PMHF [%]
R11 注 1,注 6 和注 7	2	是	开路	90%	X	SM2	99%	0.018	X	SM2	100%	0	1.782	0.3%
			短路	10%	X		99%	0.002	X		100%	0	0.198	0.0%
R12 注 1,注 6 和注 7	2	是	开路	90%	X	SM2	99%	0.018	X	SM2	100%	0	1.782	0.3%
			短路	10%	X		99%	0.002	X		100%	0	0.198	0.0%
R21 注 2	2	是	开路	90%	X	SM2	99%	0.018	X	SM2	100%	0	1.782	0.3%
			短路	10%	X		99%	0.002	X		100%	0	0.198	0.0%
R22 注 2	2	是	开路	90%	X	SM2	99%	0.018	X	SM2	100%	0	1.782	0.3%
			短路	10%	X		99%	0.002	X		100%	0	0.198	0.0%
C11 注 1,注 6 和注 7	2	是	开路	20%	X	SM2	99%	0.004	X	SM2	100%	0	0.396	0.1%
			短路	80%	X		99%	0.016	X		100%	0	1.584	0.3%
C12 注 1,注 6 和注 7	2	是	开路	20%	X	SM2	99%	0.004	X	SM2	100%	0	0.396	0.1%
			短路	80%	X		99%	0.016	X		100%	0	1.584	0.3%
C21	2	是	开路	20%		SM2				SM2				0.0%

组件名	失效率/FIT	在计算中是否考虑安全相关组件?	失效模式	失效模式分布	在缺少安全机制时失效模式是否有可能违背安全目标?	是否有防止失效模式违背安全目标的安全机制?	考虑到违背安全目标的失效模式覆盖率	残余或单点故障失效率/FIT	在结合其他组件的无关失效模式是否会违背安全目标?	探测方法? 是否有防止失效模式成为潜伏的安全机制?	考虑到潜伏失效的失效模式覆盖率	潜伏多点故障失效率/FIT	DPF_det	PMHF [%]
			短路	80%	X		99%	0.016	X		100%	0	1.584	0.3%
C22	2	是	开路	20%		SM2				SM2				0.0%
			短路	80%	X		99%	0.016	X		100%	0	1.584	0.3%
I1	4	是	开路	70%	X	SM2	99%	0.028	X	SM2	100%	0	2.772	0.5%
			短路	20%	X		99%	0.008	X		100%	0	0.792	0.1%
			漂移 0.5	5%	X		99%	0.002	X		100%	0	0.198	0.0%
			漂移 2	5%									0	0.0%
I2	4	是	开路	70%	X	SM2	99%	0.028	X	SM2	100%	0	2.772	0.5%
			短路	20%	X		99%	0.008	X		100%	0	0.792	0.1%
			漂移 0.5	5%	X		99%	0.002	X		100%	0	0.198	0.0%
			漂移 2	5%									0	0.0%
WD	20	是	输出卡滞在 1	50%					X	无	0%	10	0	0.0%
			输出卡滞在 0	50%									0	0.0%
T61	5	是	开路	50%		SM3				SM3			0	0.0%
			短路	50%	X		90%	0.25	X		100%	0	2.25	4.6%
R61 注 3 和注 6	2	是	开路	90%						无			0	0.0%
			短路	10%					X		0%	0.2	0	0.0%
R62 注 3 和注 6	2	是	开路	90%						无			0	0.0%
			短路	10%					X		0%	0.2	0	0.0%
R63 注 5	2	是	开路	90%									0	0.0%
			短路	10%									0	0.0%
R64 注 1 和注 6	2	是	开路	90%					X	无	0%	1.8	0	0.0%
			短路	10%					X		0%	0.2	0	0.0%
I61 注 5	5	否	开路	80%									0	0.0%
			短路	20%									0	0.0%

组件名	失效率/FIT	在计算中是否考虑安全相关组件?	失效模式	失效模式分布	在缺少安全机制时失效模式是否有可能违背安全目标?	是否有防止失效模式违背安全目标的安全机制?	考虑到违背安全目标的失效模式覆盖率	残余或单点故障失效率/FIT	在结合其他组件的无关失效时失效模式是否会违背安全目标?	探测方法? 是否有防止失效模式成为潜伏的安全机制?	考虑到潜伏失效的失效模式覆盖率	潜伏多点故障失效率/FIT	DPF_det	PMHF [%]
C61 注 4 和注 6	2	是	开路	20%					X	无	0%	0.4	0	0.0%
			短路	80%									0	0.0%
R81 注 5	2	否	开路	90%									0	0.0%
			短路	10%									0	0.0%
L1 注 5	10	否	开路	90%									0	0.0%
			短路	10%									0	0.0%
μC	100	是	全部	50%	X	SM4	90%	5	X	SM4	100%	0	45	91.1%
			全部	50%									0	0.0%
							Σ	5.48			Σ	12.80	69.822	99.8%

表 F.2　定量 FMEA 的结果

运行时间	10000 小时

总安全相关	157 FIT	PMHF_DPF	0.009 FIT	0.16%
总非安全相关	19 FIT	PMHF_RF	5.48 FIT	99.84%
总失效率	176 FIT	PMHF	5.489 FIT	100.00%

单点故障度量 = 1 - (5.48/157) = 96.5%
潜伏故障度量 = 1 - [12.8/(157-5.48)] = 91.6%

F.3 定义评估故障或失效模式的选择标准

一个复杂系统的安全分析工作量可能很大。确定选择标准的原则是将评估聚焦在相关的点上。在本例中，确定了以下标准：

a)　所有残余故障或单点故障 FMC≤90%的故障或失效模式。

b)　所有对总 PMHF 值贡献≥2%的故障或失效模式。

c)　对总 PMHF 值有贡献的前 20 种故障或失效模式。

注：选择标准是根据安全分析结果（例如，与目标值的偏差、贡献者的分布）确定的。

F.4 应用选择标准

表 F.3　所有残余故障或单点故障 FMC≤90%的故障或失效模式列表

ID	组件名	失效率/FIT	在计算中是否考虑安全相关组件？	失效模式	失效模式分布	防止失效模式违背安全目标的安全机制	违背安全目标的失效模式的覆盖率	对 PMHF 的贡献[FIT]	对 PMHF 的贡献[%]
45	μC	100	是	全部	0.5	SM4	90.00%	5	91.13%
28	T61	5	是	短路	0.5	SM3	90.00%	0.25	4.56%
对 PMHF 总的贡献[FIT]和[%]								5.25	95.68%

表 F.4　所有对总 PMHF 值贡献≥2%的故障或失效模式列表

ID	组件名	失效率/FIT	在计算中是否考虑安全相关组件？	失效模式	失效模式分布	防止失效模式违背安全目标的安全机制	违背安全目标的失效模式的覆盖率	对 PMHF 的贡献[FIT]	对 PMHF 的贡献[%]
45	μC	100	是	全部	0.5	SM4	90.00%	5	91.13%
28	T61	5	是	短路	0.5	SM3	90.00%	0.25	4.56%
对 PMHF 总的贡献[FIT]和[%]								5.25	95.68%

表 F.5　对总 PMHF 值有贡献的前 20 种故障或失效模式列表

PMHF 贡献	ID	组件名	失效率/FIT	在计算中是否考虑安全相关组件？	失效模式	失效模式分布	防止失效模式违背安全目标的安全机制	违背安全目标的失效模式的覆盖率	对 PMHF 的贡献[FIT]	对 PMHF 的贡献[%]
1	45	μC	100	是	全部	0.5	SM4	90.00%	5	91.13%
2	28	T61	5	是	短路	0.5	SM3	90.00%	0.25	4.56%
3	21	I2	4	是	开路	0.7	SM2	99.00%	0.028	0.51%
4	17	I1	4	是	开路	0.7	SM2	99.00%	0.028	0.51%
5	1	R11	2	是	开路	0.9	SM2	99.00%	0.018	0.33%
6	3	R12	2	是	开路	0.9	SM2	99.00%	0.018	0.33%
7	5	R21	2	是	开路	0.9	SM2	99.00%	0.018	0.33%
8	7	R22	2	是	开路	0.9	SM2	99.00%	0.018	0.33%
9	10	C11	2	是	短路	0.8	SM2	99.00%	0.016	0.29%
10	16	C22	2	是	短路	0.8	SM2	99.00%	0.016	0.29%
11	14	C21	2	是	短路	0.8	SM2	99.00%	0.016	0.29%

PMHF 贡献	ID	组件名	失效率 /FIT	在计算中是否考虑安全相关组件？	失效模式	失效模式分布	防止失效模式违背安全目标的安全机制	违背安全目标的失效模式的覆盖率	对 PMHF 的贡献 [FIT]	对 PMHF 的贡献 [%]
12	12	C12	2	是	短路	0.8	SM2	99.00%	0.016	0.29%
13		PMHF-DPF							0.00894	0.16%
14	22	I2	4	是	短路	0.2	SM2	99.00%	0.008	0.15%
15	18	I1	4	是	短路	0.2	SM2	99.00%	0.008	0.15%
16	9	C11	2	是	开路	0.2	SM2	99.00%	0.004	0.07%
17	11	C12	2	是	开路	0.2	SM2	99.00%	0.004	0.07%
18	23	I2	4	是	漂移 0.5	0.05	SM2	99.00%	0.002	0.04%
19	8	R22	2	是	短路	0.1	SM2	99.00%	0.002	0.04%
20	19	I1	4	是	漂移 0.5	0.05	SM2	99.00%	0.002	0.04%
对 PMHF 总的贡献[FIT]和[%]									5.48	99.89%

注：表 F.5 中 PMHF_DPF 表示双点失效对 PMHF 值的贡献，如表 F.2 所示。

F.5 评估与第 9 章目标的符合性

由于表 F.3 和表 F.4 中识别的故障或失效模式对 PMHF 值的贡献超过 95%，因此用这些选择标准来评估是足够的。为了评估是否符合第 9 章的目标，可以考虑下列方面：

——已经在使用的值得信赖的系统如何处理这些问题？

——处理这些问题的最新技术水平如何？

——关于所考虑的硬件要素及其故障或失效模式的现场经验是什么？

——关于所考虑的硬件要素及其故障或失效模式的可靠性评估结果是什么？

——是否有合适的专用措施（见 9.4.1.2 和 9.4.1.3）以减少在现场发生的风险？

附 录 G

（资料性）

由两个系统组成的相关项的 PMHF 预算分配示例

G.1 目标

本示例给出了跨两个系统的随机硬件失效概率度量（PMHF）预算分配流程，这两个系统均有助于实现相同的安全目标。

注：为了凸显某些流程的不足之处，本示例有所夸大。

G.2 相关项的架构

本相关项由系统 A 和系统 B 组成（见图 G.1），系统间通过车载网络总线（例如，CAN，FlexRay 或以太网）互联。

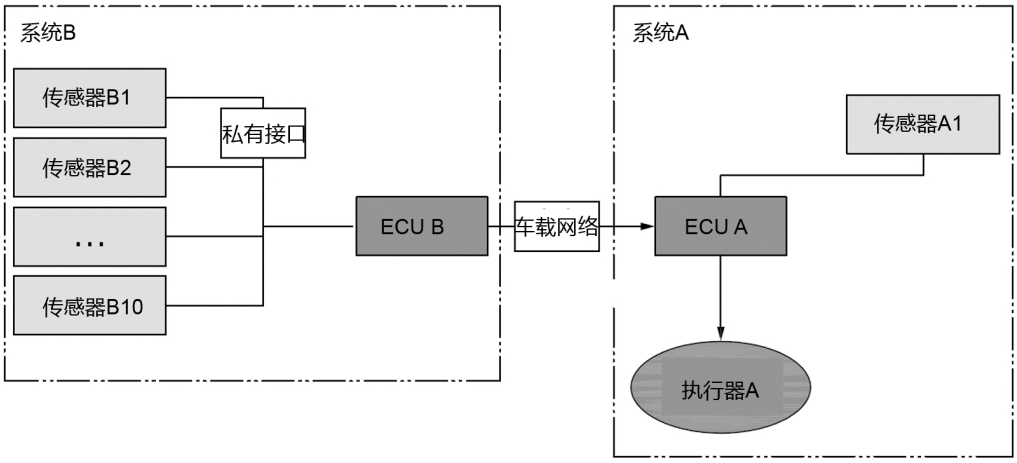


图 G.1 相关项的系统架构

系统 B 包括一个电子控制单元（ECU B）和十个传感器（传感器 B1 至传感器 B10）。系统 A 包含一个电子控制单元（ECU A）、一个传感器（传感器 A1）和一个执行器（执行器 A）。

G.3 事件链

传感器 B1 至传感器 B10 将其信号 SigB1 至 SigB10 传送至 ECU B（见图 G.2）。由 ECU B 计算出新的信号值 SigB11 至 SigB1000。ECU B 再将传感器接收到的信号 SigB1 至 SigB10、计算出新的信号值 SigB11 至 SigB1000 传送至 ECU A。

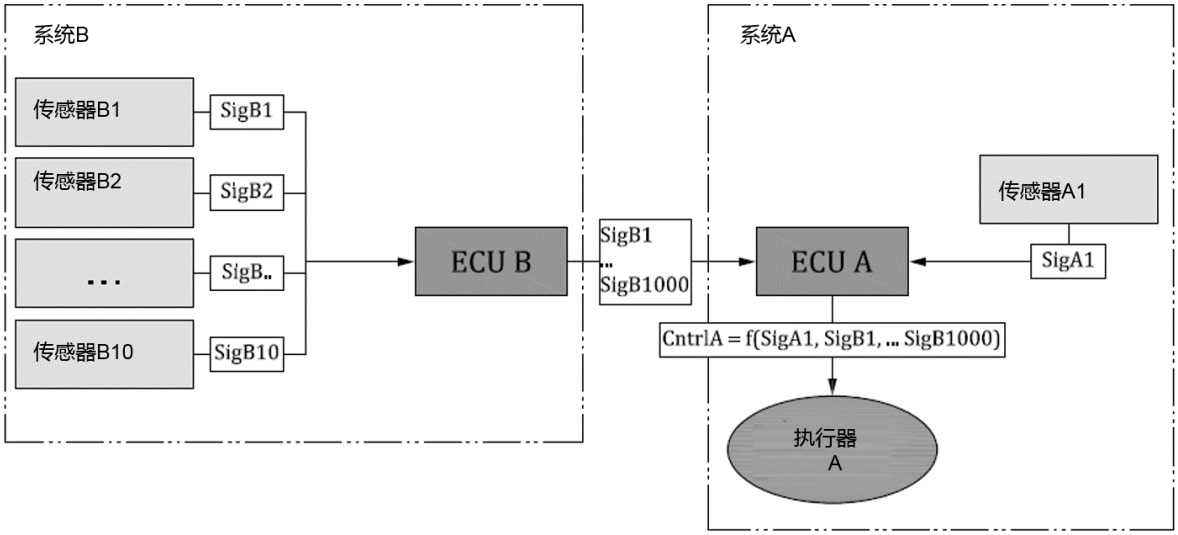


图 G.2　事件链

ECU A 根据信号 SigB1 至 SigB1000 以及传感器 A1 的信号 SigA1 计算出控制值 CntrlA，然后应用到执行器上。

G.4 条件

满足以下条件：

——安全目标 SG_A：避免执行器 A 的错误执行时长超过 100 毫秒（ASIL D 等级）；

——SigA1、SigB1 到 SigB1000 的信号值只要有一项不正确，就可能导致违背安全目标 A；

——ECU A 无法检查 SigB1 至 SigB1000 的正确性；及

——需由系统 B 检查 SigB1 至 SigB1000 的正确性。

G.5 PMHF 总体目标值

按照 9.4.2.3，PMHF 预算可能按照相关项中的系统数量进行调整。在这种情况下，两个系统和车载网络可能导致违背安全目标。每个系统分配$10^{-8}/h$ 的预算。此外，车载网络分配$10^{-10}/h$ 的预算（例如来自应用于类似设计的定量分析）。因此，违背安全目标 SG_A 所设的总预算为 2.01 $\times 10^{-8}/h$（见图 G.3）。

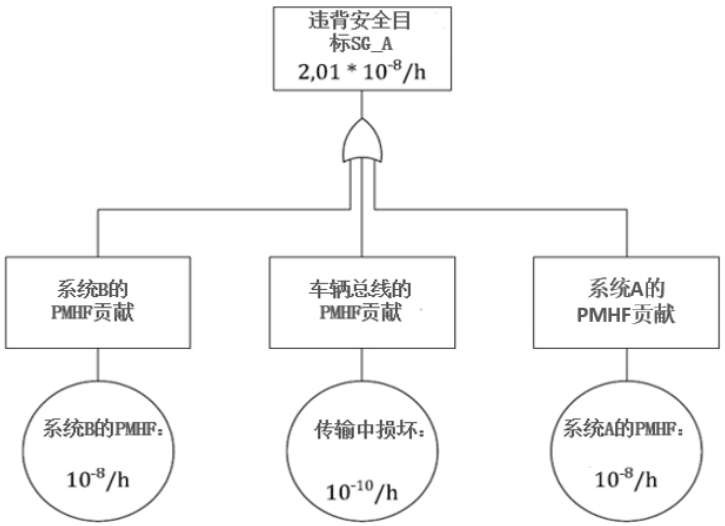


图 G.3　PMHF 目标分配

G.6 系统 B 的 PMHF 预算定义

第一步，系统 B 提供的所有信号都会被识别，这些信号可能导致违背安全目标。它们被分配到一个信号组，例如：SigGroup_SG_A = [SigB1，…，SigB1000]。

下一步，系统 B 中涉及违背安全目标 SG_A 的 PMHF 预算，会被分配给信号组 SigGroup_SG_A 中一个或多个错误的信号。

安全需求 B1：防止信号组 SigGroup_SG_A （ASIL D 等级）中一个或多个错误信号的输出：

——PMHF≤$10^{-8}/h$；

——SPFM≥99 %；

——LFM≥90 %；及

——如果一个信号与正确值的偏差≥最大值（常数，x %），则该信号被视为错误信号。

这使系统 B 的供应商可以在安全分析中识别所有相关硬件要素，并根据供应商认为合适的方式分配失效率预算（例如：图 G.4）。

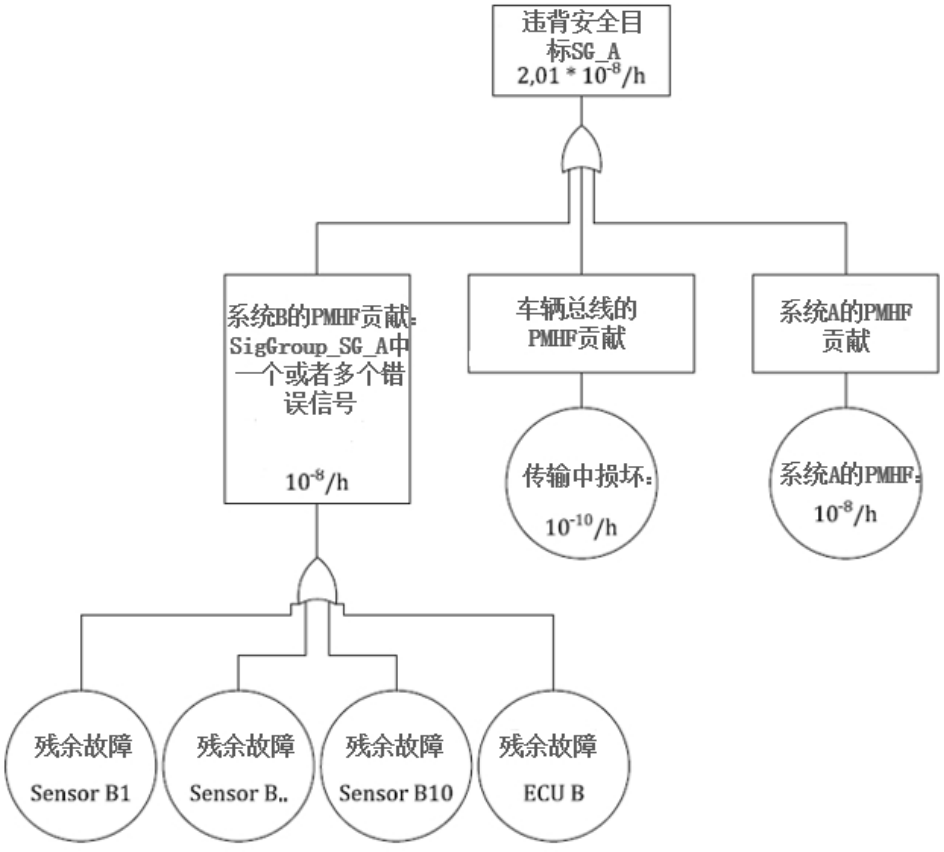


图 G.4　涉及硬件要素的 FTA

注：由于系统 B 提供的 1000 个信号中的每一个都可能违背 SG_A，并且系统 A 不能检查这些信号的正确性，因此可能会试图将系统 B 的 PMHF 预算平均分配给每个信号，这样每个信号 PMHF 预算等于$10^{-8}/1000/h = 10^{-11}/h$。在这种情况下，发给系统 A 供应商的安全要求可能会被表述为：防止输出错误的信号 Bx 值（ASIL D 等级，PMHF_SigBx≤$10^{-11}/h$，SPFM≥99%，LFM≥90%），x = 1 到 1 000。然而，系统 B 的总体 PMHF 计算中认为这些信号具有共同的硬件要素（例如 ECU B），这会导致失效率升高，并使失效不相互独立。在此示例中，每个信号均可能受到 ECU B 故障的影响，即 ECU B 中的故障可能破坏 1 至 1000 个信号。如果不考虑这一点，而将每个信号的残余失效率相加，此总数可能会高于整个系统 B 的基本失效率。因此，这种方法是不可取的。

附 录 H

（资料性）

潜伏故障处理的示例

H.1 总则

本附录旨在阐明如何处理不同类型的安全机制，并给出两个示例，以便根据 8.4.8 备选方案 a）的要求条理清晰地评估硬件度量。安全机制分为两组：基于故障探测与控制相结合的安全机制（过渡到安全状态，即使安全机制随后失效也不会有影响）和基于仅控制故障影响的安全机制。本附录还旨在阐明运用 8.4.8 中备选方案 c）仅限于执行故障探测与控制的安全机制的原因。

H.2 基于故障探测与控制的安全机制示例

在第一个示例中（见图 H.1），系统设计为具有基于故障探测与控制的安全机制：

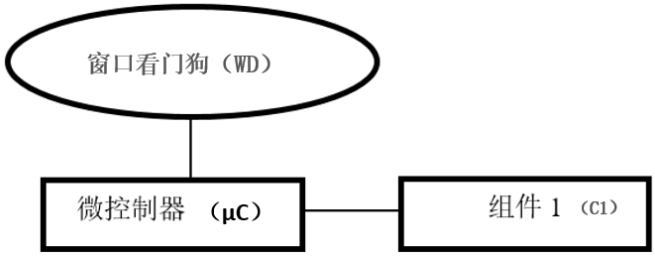


图 H.1 基于故障探测与控制的安全机制

窗口看门狗是一种监控微控制器的安全机制，其对微控制器的残余故障（例如时钟相关问题等）的诊断覆盖率为 60%。潜在违背安全目标的故障（在缺乏安全机制的情况下）中，可以被安全机制覆盖到的部分被视为可探测到的多点故障（特别是双点故障），因为安全机制探测到此故障，将其指示给驾驶员，防止违背安全目标（即故障受控）。一旦窗口看门狗探测到故障，它将使系统过渡到安全状态。

如果窗口看门狗发生故障，那么可能失去对微控制器失效模式的探测或错误控制能力。如果这个故障既没有被安全机制探测到（窗口看门狗启动测试），也没有被司机感知到（假设受到窗口看门狗故障的影响，驾驶员不可能获悉故障），那么此故障被视为潜伏故障。

考虑到上述提及的分类，下表是描述硬件度量评估的定量分析摘录：

表 H.1 基于故障探测与控制的安全机制定量分析摘录

组件名	失效模式	失效率 λ	是否有可能直接违背安全目标？	是否有防止失效模式违背安全目标的安全机制？	诊断覆盖率	残余故障失效率	结合其他故障是否会违背安全目标？	是否有防止失效模式成为潜伏的安全机制？	考虑到潜伏失效的失效模式覆盖率	潜伏故障失效率
微控制器（μC）	时钟相关问题	100 FIT	是	窗口看门狗	60%	40 FIT	是	窗口看门狗	100%	0
窗口看门狗（WD）	失效	40 FIT	否	—	—	—	是	窗口看门狗启动测试	90%	4 FIT

组件 1（C1）	失效	50 FIT	是	微控制器（μC）	97%	1.5FIT	是	微控制器（μC）	100%	0
…										

注 1：8.4.8 的备选方案 c）可适用于每一个安全机制都是基于故障探测与控制的系统，其安全机制的失效可能导致违背安全目标。在这种情况下，备选方案 c）是有效的，因为安全机制监测的失效模式不会影响潜伏故障 FIT。因此，安全机制对潜伏故障 FIT 的唯一贡献来自安全机制本身。

注 2：微控制器的失效模式（时钟相关问题—100FIT）可能会违背安全目标。窗口看门狗是合适的控制时钟相关故障的安全机制。窗口看门狗的失效与另一个故障相结合可能违背安全目标。将看门狗启动测试未探测到的窗口看门狗故障视为潜伏故障（4FIT）。安全机制会防止 60%（60FIT）的微控制器失效模式违背安全目标，因此与残余故障相关的失效率为 40FIT。合适的安全机制（窗口看门狗）可以探测 60%已考虑的失效模式（60FIT），该安全机制探测故障并触发到安全状态的过渡，从而防止违背安全目标。按照 GB/T34590.10-XXXX 中随机硬件故障的分类，安全机制所覆盖的故障（60FIT）被视为探测到的多点故障，因此不能将其定义为潜伏故障。

注 3：组件 1 中的故障通过微控制器来控制，诊断覆盖率为 97%。

上述论据仅适用于基于故障探测与控制的安全机制。对于基于故障影响控制的安全机制，该论据无效（例如，不上报错误信号的 RAM 的 EDC）。

H.3 基于故障影响控制的安全机制示例

在第二个示例中（见图 H.2），系统设计为具有基于故障影响控制的安全机制。

图 H.2　基于故障影响控制的安全机制

在此图示中（图 H.2）： A = 组件 A； 滤波器 = 离散组件；B = 组件 B。

安全要求是“系统必须提供符合其电气规范的信号”，违背此安全要求可能导致违背安全目标。

注 1：假定在无故障条件下组件 A 提供正确的信号。

如果故障发生在组件 A，使得 A 提供的信号被干扰，出现噪声，噪声会被安全机制（滤波器）过滤掉。因此，如果信号显示出持续的噪声，由于滤波器工作正常，它将及时地被滤波器恢复为正常信号。针对失效模式“信号噪声”，合适的安全机制的失效模式覆盖率为 99.9%。由于在此情况下，即合适的安全机制执行持续且准时的恢复，在缺少安全机制的情况下潜在违背安全目标的故障受到控制，但是该故障既不会被探测到也不会被感知到；因此这种故障被视为潜伏故障。

一旦组件 A 已经发生永久性故障，当滤波器也发生故障时双点失效就产生了；在此之前，被覆盖的组件 A 的故障将无法在系统层面体现。

注 2：像示例中所示的滤波器那样的安全机制并不执行故障探测，而仅控制故障。因此，此系统不能够区分功能故障和正常行为（安全机制的动作持续被触发，直到安全机制本身发生失效）。

表 H.2　基于故障影响控制的安全机制定量分析摘要

组件名	失效模式	失效率λ	是否有可能直接违背安全目标？	是否有防止失效模式违背安全目标的安全机制？	诊断覆盖率	残余故障失效率	结合其他故障是否会违背安全目标？	是否有防止失效模式成为潜伏的安全机制？	对潜伏失效的故障机制覆盖率	潜伏故障失效率
A	信号噪声	100 FIT	是	滤波器	99.9%	0.1 FIT	是	否	0%	99.9FIT
滤波器	失效	40 FIT	否	—	—	—	是	否	0%	40 FIT
B	失效	20 FIT	是	—	0%	20 FIT	—	—	—	—
…										

注 3：8.4.8 的备选方案 c）不适用于具有基于故障影响控制的安全机制特征的系统。因此，在此情况下 8.4.8 的备选方案 a）和 b）是仅有的可选择项。

参 考 文 献

[1] ISO 7637-2, Road vehicles — Electrical disturbances from conduction and coupling — Part 2: Electrical transient conduction along supply lines only.

[2] ISO 7637-3, Road vehicles — Electrical disturbances from conduction and coupling — Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines.

[3] ISO 10605, Road vehicles — Test methods for electrical disturbances from electrostatic discharge.

[4] ISO 11452-2, Road vehicles — Component test methods for electrical disturbances from narrowband radiated electromagnetic energy — Part 2: Absorber-lined shielded enclosure.

[5] ISO 11452-4, Road vehicles — Component test methods for electrical disturbances from narrowband radiated electromagnetic energy — Part 4: Harness excitation methods.

[6] ISO 16750-2, Road vehicles — Environmental conditions and testing for electrical and electronic equipment — Part 2: Electrical loads.

[7] ISO 16750-4, Road vehicles — Environmental conditions and testing for electrical and electronic equipment — Part 4: Climatic loads.

[8] ISO 16750-5, Road vehicles — Environmental conditions and testing for electrical and electronic equipment — Part 5: Chemical loads.

[9] GB/T 20438-2017（所有部分） 电气/电子/可编程电子安全相关系统的功能安全.

[10] IEC 61709, Electronic components — Reliability — Reference conditions for failure rates and stress models for conversion.

[11] SN 29500 (2004), Siemens AG, Failure Rates of Components — Expected Values, General

[12] （空白）

[13] EN 50129:2003, Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling.

[14] MIL HDBK 217 F notice 2, Military handbook: Reliability prediction of electronic equipment.

[15] MIL HDBK 338, Military handbook: Electronic reliability design handbook.

[16] NPRD-2016, Non-electronic Parts Reliability Data.

[17] RIAC FMD-2016. Failure Mode / Mechanism Distributions.

[18] RIAC HDBK 217 Plus, Reliability Prediction Models.

[19] UTE C80-811, Reliability methodology for electronic systems.

[20] BIROLINI. A., Reliability Engineering, Theory and Practice, 2014.

[21] Sundaram P., & D ’ Ambrosio J.G. Controller Integrity in Automotive Failsafe System Architectures, SAE 2006 World Congress, 2006-01-0840.

[22] Fruehling T., & D elphi Secured Microcontroller Architecture S.A.E. 2000 World Congress, SAE# 2000- 01- 1052.

[23] Mahmood A., & McCluskey E.J.“ Concurrent Error Detection Using Watchdog Processors - A Survey”, IEEE Trans. Computers, 37(2), 160-174 (1988).

[24] Leaphart E., C zerny B., D ’ Ambrosio J. Survey of Software Failsafe Techniques for Safety-Critical Automotive Applications, SAE 2005 World Congress, 2005-01-0779.

[25] Mariani R ., F uhrmann P ., Vittorelli B. Cost-effective Approach to Error Detection for an Embedded Automotive Platform, 2006-01-0837, SAE 2006 World Congress & Exhibition, April 2006, Detroit, MI, USA.

[26] Patel J., & F ung L.“ Concurrent Error Detection in ALU’s by Recomputing with Shifted Operands”, IEEE Transactions on Computers, Vol. C-31, pp.417-422, July 1982.

[27] Forin P. Vital Coded Microprocessor: Principles and Application for various Transit Systems, Proc. IFAC-GCCT, Paris, France, 1989.

[28] Ramabadran T.V., & Gaitonde S.S. 1988),“ A tutorial on CRC computations”. IEEE Micro 8 (4):62 - 75, 1988.

[29] Koopman P., & Chakravarty T. 2004), Cyclic Redundancy Code (CRC) Polynomial Selection for Embedded Networks The International Conference on Dependable Systems and Networks, DSN-2004, http: //www .ece .cmu .edu/ ~koopman/roses/dsn04/koopman04 crc poly embedded .pdf.

[30] FIDES guide 2009 edition A (September 2010), Reliability Methodology for Electronic Systems.