ICS

T

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

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

（征求意见稿）

2016.01.15

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

GB/T XXXXX《道路车辆 功能安全》包括十个部分：

——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：生产和运行；

——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。

本部分为GB/T XXXXX的第5部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分修改采用国际标准ISO 26262-5：2011 《道路车辆 功能安全 第5部分：产品开发：硬件层面》（英文版）。

本部分的附录A、B、D、E、F为资料性附录,附录C为规范性附录。

本部分由国家标准化管理委员会提出。

本部分由全国汽车标准化技术委员会（SAC/TC114）归口。

本部分起草单位：

本部分主要起草人：

引　言

ISO 26262 是以 IEC61508 为基础，为满足道路车辆上特定电子电气系统的需求而编写。

ISO 26262 适用于道路车辆上特定的由电子、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。

安全是未来汽车发展的关键问题之一，不仅在驾驶辅助和动力驱动领域，而且在车辆动态控制和主被动安全系统领域，新的功能越来越多地触及到系统安全工程领域。这些功能的开发和集成将强化对安全相关系统开发流程的需求，并且要求提供满足所有合理的系统安全目标的证明。

随着技术日益复杂、软件内容和机电一体化应用不断增加，来自系统性失效和硬件随机失效的风险逐渐增加。ISO 26262 通过提供适当的要求和流程来避免风险。

系统安全是通过一系列安全措施实现的。安全措施通过各种技术（例如，机械、液压、气压、电子、电气、可编程电子等）实现且应用于开发过程中的不同层面。尽管 ISO 26262 针对的是电子电气系统的功能安全，但是它也提供了一个基于其它技术的与安全相关系统的框架。ISO 26262：

a) 提供了一个汽车安全生命周期(管理、开发、生产、运行、维护、报废)，并支持在这些生命周期阶段内对必要活动的剪裁；

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；

c) 应用汽车安全完整性等级规定 ISO 26262 中适用的要求，以避免不合理的残余风险；

d) 提供了对于确认和认可措施的要求，以确保达到一个充分、可接受的安全等级；

e) 提供了与供应商相关的要求。

功能安全受开发过程(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、维护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开发活动和工作成果相互关联。ISO 26262 涉及与安全相关的开发活动和工作成果。

图1为ISO 26262的整体架构。ISO 26262基于V模型为产品开发不同阶段提供过程参考：

— 阴影"V"表示标准中第 3、4、5、6 和 7 部分之间的关系；

— 以“m-n”方式表示的具体条款中，“m”代表特定部分的编号，“n”代表该部分章条的编号。

示例：“2-6”代表 GB/TXXXX-2 的第六章

图1 GB/T XXXXX概览

道路车辆 功能安全

第5部分：产品开发：硬件层面

1 范围

GB/T XXXXX适用于安装在最大总质量不超过3.5吨的量产乘用车上的包含一个或多个电子电气系统的与安全相关的系统。

GB/T XXXXX不适用于安装在特殊用途车辆上的特定的电子电气系统，例如为残疾驾驶者设计的车辆。

已经完成生产发布的系统及其组件或在本标准发布日期前开发的系统及其组件不适用于本标准。对于在本标准发布前完成生产发布的系统及其组件进行进一步的开发或变更时，仅修改的部分需要按照本标准开发。

本标准针对由电子电气安全相关系统的故障行为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。本标准不针对与触电、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，除非危害是直接由电子电气安全相关系统的故障行为而引起的。

本标准不针对电子电气系统的标称性能，即使这些系统（例如主动和被动安全、制动系统、自适应巡航系统）有专用的功能性能标准。

本部分规定了车辆在产品开发硬件层面的要求，包括：

— 启动产品开发硬件层面的要求，

— 硬件安全要求的定义，

— 硬件设计，

— 硬件架构度量，及

— 因随机硬件失效导致违背安全目标的评估，硬件集成及测试。

本部分对于硬件要素的要求适用于非可编程和可编程要素，如ASIC，FPGA和PLD。而且，GB/T XXXXX-6，GB/T XXXXX-8的第11章和12章中的要求对于可编程电子要素是适用的。

2 规范性引用文件

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

GB/T XXXXX-1:201X，道路车辆 功能安全 第1部分：术语；

GB/T XXXXX-2:201X，道路车辆 功能安全 第2部分：功能安全管理；

GB/T XXXXX-4:201X，道路车辆 功能安全 第4部分：产品开发：系统层面；

GB/T XXXXX-6:201X，道路车辆 功能安全 第6部分：产品开发：软件层面；

GB/T XXXXX-7:201X，道路车辆 功能安全 第7部分：生产和运行；

GB/T XXXXX-8:201X，道路车辆 功能安全 第8部分：支持过程；

GB/T XXXXX-9:201X，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；

3 术语、定义和缩略语

GB/T XXXXX-1给出的术语、定义和缩略语适用于本部分。

4 要求

4.1 一般要求

如声明满足GB/T XXXXX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 的要求，已经计划安全活动的剪裁并表明这些要求不适用，或，

b) 不满足要求的理由存在且可接受的，并且按照 GB/T XXXXX-2 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。上一阶段工作成果作为“前提条件”的这一信息应具备。如果条款的某些要求是依照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，但在某些案例中，GB/T XXXXX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。

4.2 对表格的诠释

表属于规范性表还是资料性表取决于上下文。在实现满足相关要求时，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（在最左侧栏以顺序号标明，如 1,2,3），或

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

对于连续的条目，全部方法应按照ASIL等级推荐予以使用。除了所列出的方法外，如果应用所列出方法以外的其它方法，应给出满足相关要求的理由。

对于选择性的条目，按照ASIL等级指示的要求，应采用适当的方法组合，不依赖于组合的方法是否在表中列出。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，则应采用具有更高推荐等级的方法。应给出组合方法满足相关要求的理由。

注：在表中所列出的方法的理由是充分的。但是，这并不意味着有偏袒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，未推荐或反对该方法。

4.3 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，应满足每一子章条的要求或建议。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 XXXXX中ASIL等级在括号中给出，则对于该ASIL等级，相应的子章节应被认为是推荐而非要求。这里的括号与ASIL等级分解无关。

5 启动硬件层面产品开发

5.1 目的

启动产品开发的硬件层面的目的是确定并计划硬件开发各子阶段过程中的功能安全活动，也包括在GB/T XXXXX-8中所描述的必要的支持过程。

硬件特定的安全活动的计划包含在安全计划中（参见GB/T XXXXX-2,6.4.3和GB/T XXXXX-4,5.4）。

5.2 总则

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阐明了为满足本部分要求的产品开发硬件层面的流程步骤，以及GB/T XXXXX框架内这些步骤的集成。

产品开发硬件层面的必要活动和流程包括：

— 技术安全概念的硬件实现；

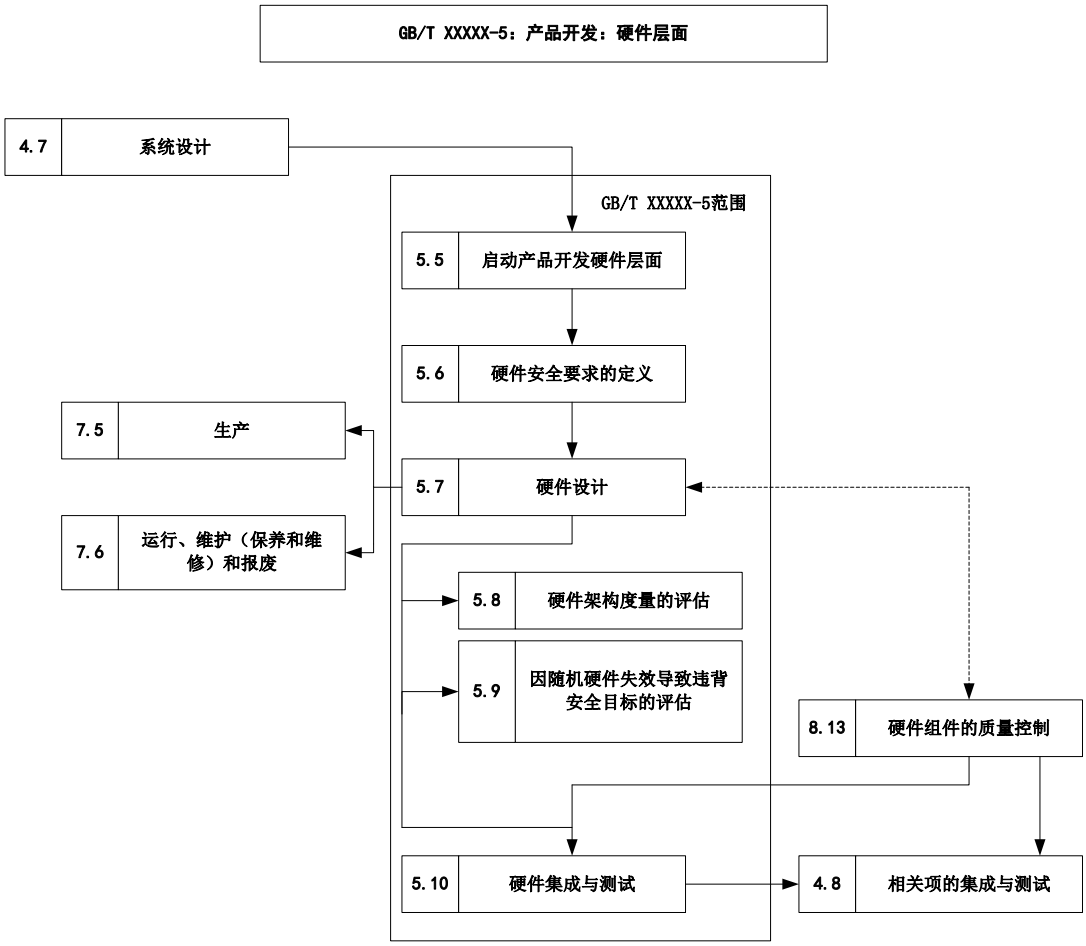
— 分析潜在硬件故障及其影响；及

— 与软件开发的协调。

与软件开发子阶段相比，本部分包含两个章节来描述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章描述了两个可选的方法以评估违背安全目标的残余风险是否足够低，或者应用一种全局概率方法，或者应用一种割集分析方法，来研究硬件要素中所识别出的每个故障对违背安全目标的影响。



注：在图中，GB/T XXXXX的各部分具体条款用以下列方式来表明：“m-n”，其中“m”代表“部分”的编号和“n”表示“章”的编号，例如，“4-5”表示GB/T XXXXX的第4部分的第5章。

图 2 产品开发硬件层面参考阶段模型

5.3 本章的输入

5.3.1 前提条件

应具备下列信息：

— 项目计划（细化的），按照 GB/T XXXXX-4,5.5.1；

— 安全计划（细化的），按照 GB/T XXXXX-4,5.5.2；

— 相关项集成和测试计划（细化的），按照 GB/T XXXXX-4,5.5.3。

5.3.2 支持信息

可考虑下列信息：

— 鉴定报告（硬件组件或元器件），如果适用（见 GB/T XXXXX-8,13.5.3）。

5.4 要求和建议

5.4.1 应细化按照 GB/T XXXXX-2 所制定的安全计划，包括产品开发硬件层面活动的适当方法和措施的确定，与 GB/T XXXXX-6 中活动的计划保持一致。

5.4.2 相关项硬件的开发流程，包括方法和工具，应在硬件开发的所有子阶段内保持一致，并与系统和软件子阶段保持一致，以便在硬件开发过程中保持要求流的精确性和一致性。

5.4.3 产品开发硬件层面的安全生命周期活动的剪裁应按照 GB/T XXXXX-2，6.4.5 实施，并基于图 2 给出的参考阶段模型。

5.4.4 应识别出对硬件组件的复用，或对经过认可的硬件组件或元器件的使用，并且应描述由此产生的对安全活动的剪裁。

5.5 工作成果

5.5.1 **安全计划**（细化的），由 5.4.1-5.4.4 的要求得出。

6 定义硬件安全要求

6.1 目的

本章的第一个目的是定义硬件安全要求，这些要求由技术安全概念和系统设计规范导出。

第二个目的是验证硬件安全要求与技术安全概念及系统设计规范的一致性。

本阶段另一目的是细化最初在GB/T XXXXX-4第7章定义的软硬件接口（HSI）规范。

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：

— 安全计划（细化的），按照5.5的要求；

— 技术安全概念，按照GB/T XXXXX-4，7.5.1；

— 系统设计规范，按照GB/T XXXXX-4，7.5.2； 及

— 软硬件接口规范，按照GB/T XXXXX-4，7.5.3。

6.3.2 支持信息

可考虑如下信息：

— 软件安全需求规范（参见GB/T XXXXX-6, 6.5.1）。

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。

6.4.2 硬件安全需求规范应包括与安全相关的每一条硬件要求，包括以下：

注1：a)、b)、c)或d)中描述的硬件安全要求包括确保其安全机制有效性所需的特性。

a) 为控制要素硬件内部失效的安全机制的硬件安全要求和相关属性，这包括用来覆盖相关瞬态故障(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：属性可包括看门狗的定时和探测能力。

b) 为确保要素对外部失效容错的硬件安全要求和安全机制的相关属性。

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) 为符合其它要素的安全要求的硬件安全要求和安全机制的相关属性；

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及安全机制的相关属性；及

注2：d)项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) 没有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。

6.4.3 此要求适用于等级为 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 XXXXX-4 第 7 章的要求，为本部分第 8 章规定的度量设定的目标值。

注：在GB/T XXXXX-8第5章定义的分布式开发情况下，此活动可包括目标值的拆分。

6.4.4 此要求适用于等级为 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 XXXXX-4 第 7 章的要求，为本部分第 9 章规定的流程设定的目标值。

注:在GB/T XXXXX-8第5章定义的分布式开发情况下，此活动可包括目标值的拆分。

6.4.5 硬件安全要求应按照 GB/T XXXXX-8 第 6 章的要求进行定义。

6.4.6 应定义相关项或要素的硬件设计验证准则，包括环境条件（温度、振动、EMI 等），特定的运行环境（供电电压、任务概述等）以及特定于组件的要求：

a) 对于中等复杂性的硬件组件或元器件的鉴定验证，其准则应满足GB/T XXXXX-8第13章的需求。

b) 通过测试进行的验证，其准则应满足第10章的需求。

6.4.7 硬件安全要求应符合 GB/T XXXXX-4 中 6.4.2.3 要求制定的安全机制的故障容错时间间隔。

6.4.8 硬件安全要求应符合 GB/T XXXXX-4 中 6.4.4.2 要求制定的多点故障探测时间间隔。

注1：对于ASIL级别为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可以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可以通过对随机硬件失效的发生概率的定量分析来确定。

6.4.9 硬件安全要求应按照 GB/T XXXXX-8 第 6 章和第 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) 关于分配给硬件要素的技术安全要求的完整性；

c) 与相关软件安全要求的一致性；及

d) 正确性与精确性。

6.4.10 在 GB/T XXXXX-4 第 7 章中最初定义的软硬件接口（HSI）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 负责硬件和软件开发的人员同时也应共同负责验证细化后的软硬件接口（HSI）规范的充分性。

6.5 工作成果

6.5.1 **硬件安全需求规范（包括测试和认可准则）**，由 6.4.1 到 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 和 6.4.11 的要求得出。

注：此工作成果可以参考GB/T XXXXX-6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 的要求得出。

7 硬件设计

7.1 目的

本章的第一个目的是按照系统设计规范和硬件安全要求设计硬件。

本章的第二个目的是验证硬件设计是否违背系统设计规范和硬件安全要求。

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单一的硬件设计，在此子阶段，安全和非安全性要求应在同一开发过程中处理。

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；

— 硬件与软件接口规范（细化的），按照6.5.2；

— 系统设计规范，按照GB/T XXXXX-4，7.5.2；及

— 安全计划（细化的），按照5.5。

7.3.2 支持信息

可考虑下列信息：

— 软件安全需求规范（参见GB/T XXXXX-6，6.5.1）。

7.4 要求和建议

7.4.1 硬件架构设计

7.4.1.1 硬件架构应执行第 6 章定义的硬件安全要求。

7.4.1.2 每个硬件组件应继承其所执行的硬件安全要求中最高的 ASlL 等级。

注：硬件组件的各个特征将继承该组件所执行的硬件安全要求中最高的ASlL 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 分解，ASIL 分解应按照 GB/T XXXXX-9, 第 5 章的要求进行。

7.4.1.4 如果一个硬件要素由指定为不同 ASlL 等级的子要素组成，或由没有指定 ASIL 等级及安全相关的子要素组成。除非满足按照 GB/T XXXXX-9 的共存准则，否则每个子要素应当按照最高 ASIL 等级处理。

7.4.1.5 在硬件安全要求和其执行之间的可追溯性，应保持到硬件组件的最底层。

注：可追溯性不要求深入到硬件详细设计，而且不需要为硬件元器件指定ASIL等级。

7.4.1.6 为了避免高复杂性导致的失效，硬件架构设计应该通过使用表 1 中列出的原则，以具有下述特性：

a) 模块化；

b) 适当的粒度水平；及

c) 简单性。

表 1 模块化的硬件设计特性

特性	ASIL			
	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、来自硬件架构的其它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 XXXXX-2, 5.4.2.7，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零部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、来自硬件组件的其它硬件元器件或其所在环境的串扰。

7.4.2.3 硬件详细设计中，硬件元器件的运行条件应符合它们的环境和运行限制规范。

7.4.2.4 应考虑鲁棒性设计原则。

注：鲁棒性设计原则可利用基于质量管理方法的核对表来展示。

示例：保守的组件规范。

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 XXXXX-9，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，安全分析可用于硬件设计验证（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

		A	B	C	D
1	演绎分析 [a]	o	+	++	++
2	归纳分析 [b]	++	++	++	++
注： 分析的详细程度和设计的详细程度是相称的。在某些情况下，两种方法都可在不同的细节层面上执行。					
[a] 一个典型的演绎分析方法是 FTA。 [b] 一个典型的归纳分析法是 FMEA。					

7.4.3.2 此要求适用于等级为 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：在大多数情况下，分析可以限制到双点故障。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）。

注2：识别双点故障的目的，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)。

7.4.3.3 此要求适用于等级为 ASIL (B)、C 和 D 的安全目标。应具备安全机制避免单点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保持安全状态或安全的切换到安全状态的能力(特别是在容错时间间隔内适当的失效减轻能力）；及

b) 应评估残余故障的诊断覆盖率。

注1：一个可在任何时间（例如不仅在上电时）发生的故障，如果诊断测试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，则不能认为此故障被有效覆盖。

注2：如果可以证明故障仅发生在上电时，并且在车辆行驶期间发生的概率是可以忽略的，那么这些故障仅在上电后执行启动测试是可以接受的。

注3：可用比如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，这种评估可以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5：附录D可作为诊断覆盖率（DC）的起始点，此起点是声明的有合适理由支持的诊断覆盖率。

7.4.3.4 此要求适用于等级为ASIL (B)、C和D的安全目标。应具备安全机制避免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及警示驾驶员的能力，以确定哪些故障保持潜伏，哪些故障不再保持潜伏；及

b) 应评估潜伏故障的诊断覆盖率。

注1：如果一个故障的诊断测试时间间隔加上相应安全机制的故障响应时间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：可用比如FMEA或FTA分析来构建理由。

注3：附录D可作为诊断覆盖率（DC）的起始点，此起点是声明的有合适理由支持的诊断覆盖率。

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，这种评估可以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。

7.4.3.5 如果适用，应按照GB/T XXXXX-9第7章进行的关联失效分析，提供证据证明硬件设计与它们的独立性要求相符合。

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安全目标覆盖，则应按照GB/TXXXXX-8中的变更管理流程对它们进行危害分析和风险评估。

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 XXXXX 范围之外，但在危害分析和风险评估中可对它们添加如下注释，“由于不在GB/T XXXXX”的范围内，所以没有对该危害指定ASIL等级”。然而，也可以指定一个ASIL等级作参考。

7.4.4 硬件设计验证

7.4.4.1 应按照 GB/T XXXXX -8第9章来验证硬件设计与硬件安全要求的一致性和完整性。为达到这一目的，应考虑表3中列出的方法。

表3 硬件设计验证

方法		ASIL			
		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	+	+	+
注:该验证评审的范围是硬件设计的技术正确性。					
[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（例如作为故障注入技术）。					

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执行是不可行的，应按照 GB/T XXXXX-8 中的变更管理流程提出变更请求。

7.4.5 生产、运行、维护和报废

7.4.5.1 如果安全分析表明生产、运行、维护和报废与安全相关，则应定义其安全相关的特殊特性，这些特殊特性应包括如下属性：

a) 生产和运行的验证措施；及

b) 这些措施的接受准则。

示例：一种依赖于新的传感器技术的硬件设计的安全性分析（例如，影像或雷达传感器），可以揭示与这些传感器要求的特殊安装流程的关系。在这种情况下，这些组件的额外验证措施有必要在生产阶段进行。

7.4.5.2 如果对安全相关硬件要素的组装、拆卸和报废可能影响技术安全概念，则应定义这些操作的指导说明。

7.4.5.3 应按照 GB/T XXXXX-7, 5.4.1.2 确保安全相关硬件要素的可追溯性。

注：这可以包括适当的标签或其它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 如果维护可能影响技术安全概念，应定义安全相关硬件要素的维护说明。

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、维护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

本章的目的是用表征故障处理要求的硬件架构度量来评估相关项的硬件架构。

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适用于相关项中的整体硬件，并且用于补充第9章描述的对随机硬件故障导致的违背安全目标的评估。

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：计算中可忽略阶次高于2的多点故障硬件要素，除非它们与技术安全概念相关

硬件架构度量可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：度量是可核实的，并且足够精确以区分不同的架构；

—支持最终设计的评估（基于详细的硬件设计完成精确计算）；

— 为硬件架构提供依据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，可以为供应商的硬件要素分配目标值。

示例：为方便分布式开发，可为微控制器或者ECU分配目标值。

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；

— 硬件安全分析报告，按照7.5.2。

8.3.2 支持信息

可考虑下列信息：

— 技术安全概念（参见GB/T XXXXX-4, 7.5.1）；及

— 系统设计规范（参见GB/T XXXXX-4, 7.5.2)。

8.4 要求和建议

8.4.1 此要求适用于等级为 ASIL (B)、C 和 D 的安全目标。应将符合附录 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 至 8.4.9 的要求。

8.4.2 此要求适用于等级为 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：为此目的，可使用表 D.1 至 D.14 作为起点，此起点是声明的有合适理由支持的诊断覆盖率。

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，这种评估可以是一个硬件要素的全局诊断覆盖率评估，或更详细的失效模式的覆盖率评估。

8.4.3 此要求适用于等级为 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：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 IEC/TR 62380, IEC 61709, MIL HDBK 217 F notice 2, RIAC HDBK 217 Plus, UTE C80-811, NPRD 95, EN 50129:2003, Annex C, IEC 62061:2005, Annex D, RIAC FMD97 和 MIL HDBK 338。

注 1：这些数据库给出的失效率数据一般都比较保守。

b) 使用现场反馈或测试的统计数据。这种情况下，预估的失效率宜有合适的置信度，或

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。专家判断应依据结构化准则进行，这些准则是判断的基础，应在失效率预估前进行设定。

注 2：专家判断准则可包括现场经验、测试、可靠性分析和设计的新颖性。

8.4.4 此要求适用于等级为 ASIL (B)、C 和 D 的安全目标。如果没有充分的证据证明计算出的单点故障或潜伏故障的失效率的可靠性，应提出替代方案（例如，增加安全机制来探测和控制此故障）。

注：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。

8.4.5 此要求适用于等级为 ASIL (B)、C 和 D 的安全目标。对于每一个安全目标，由 GB/T XXXXX-4 7.4.4.2 要求的“单点故障度量”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原则中，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 此要求适用于等级为 ASIL (B)、C 和 D 的安全目标。对于每一个安全目标，由 GB/T XXXXX-4 7.4.4.2 要求的“潜伏故障度量”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原则中，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 此要求适用于等级为 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（在8.4.5中给出），并有理由说明在硬件要素层符合这些目标。

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/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值有助于规避这种不良影响。

注 2：当显示瞬态故障与，例如，所用技术相关时，要考虑这些瞬态故障。可以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 中所解释的），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 4.1 所述评估如何实现安全目标的理由。

注 4：可以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。

8.4.8 此要求适用于等级为 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符合这些目标。

c) 对于其故障可导致安全机制（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（被当做诊断覆盖率），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。在其它情况下，则只有选项 a)和 b)适用。

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/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值有助于规避这种不良影响。

注 4：如果不满足目标，将按 4.1 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伏故障度量；但在这种情况下，采用最高 ASIL 等级的安全目标的度量目标。

8.4.9 此要求适用于等级为 ASIL (B)、C 和 D 的安全目标。应按照 GB/T XXXXX-8 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：仔细验证单点故障度量，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的分析，由 8.4.1 至 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

本章中要求的目的是制定可用的准则，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。

注：“足够低”指“与已经在使用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，也可考虑多点故障。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。

第一个方法包括使用概率的度量，即“随机硬件失效概率度量”（PMHF），通过使用例如定量故障树分析（FTA）及将此计算结果与目标值相比较的方法，评估是否违背所考虑的安全目标。

第二个方法包括独立的评估每个残余和单点故障，及每个双点失效是否导致违背所考虑的安全目标。此分析方法也可被考虑为割集分析。

注：在可靠性分析中，故障树中的一个割集是一组基本事件，其发生导致顶层事件的发生。

所选用的方法在硬件架构设计和硬件详细设计中可以被迭代应用。

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

可考虑下列信息：

— 技术安全概念（参见GB/T XXXXX-4，7.5.1）；及

— 系统设计规范（参见GB/T XXXXX-4，7.5.2）

9.4 要求和建议

9.4.1 总则

此要求适用于等级为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。

9.4.2 随机硬件失效概率度量（PMHF）的评估

9.4.2.1 此要求适用于等级为ASIL(B)、C和D的安全目标。应按照GB/T XXXXX-4，7.4.4.3的要求，为随机硬件失效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原则的现场数据，或
c) 来自应用于值得信赖的相似设计原则中的定量分析技术(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。

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	$<10^{-8}\,h^{-1}$
C	$<10^{-7}\,h^{-1}$
B	$<10^{-8}\,h^{-1}$
注：此表中描述的定量目标值可按照 4.1 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）。	

9.4.2.2 此要求适用于等级为 ASIL(B)、C 和 D 的安全目标。9.4.2.1 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。

9.4.2.3 此要求适用于等级为 ASIL(B)、C 和 D 的安全目标。针对单点、残余和双点故障的硬件架构定量分析，应提供证据证明 9.4.2.1 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) 每个可导致双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) 双点故障情况下的暴露持续时间。

注 1：在定量分析中，考虑可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。它们可以是单点故障、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：

a) 与每个安全机制有关的多点故障探测时间区间，或者当故障不对驾驶员显示（潜伏故障）时的车辆生命周期；
b) 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
c) 直到车辆进入车间维修前的平均时间区间（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，它可以短至几毫秒。当没有监控时，它可以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区间可以被认为是等于 1 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：对使用集成诊断的安全机制，可用表 D.1 至 D.14 作为出发点，用声明的有合适理由支持的诊断覆盖率去评估这些安全机制的诊断覆盖率。

注 5：相关项处于下电模式的情况不包含在每小时平均概率的计算中，由此防止人为的降低每小时的平均概率。因此，对于每天仅运行 1 小时的相关项，剩余的 23 小时不在此运行目标值的计算中考虑。

注 6：如果目标没有被满足，应按 4.1 对给出的如何达到安全目标的理由进行评估。

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，评估可以是硬件要素的全局诊断覆盖率，或者更详细失效模式覆盖率的评估。

9.4.2.4 此要求适用于等级为 ASIL C 和 D 的安全目标。仅在已采取专用措施的情况下，才应认为硬件元器件发生的单点故障是可接受的。

注：专用措施可包括：

a) 设计特征，如硬件元器件过设计（例如，电气或热压力等级）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。

9.4.2.5 此要求适用于等级为 ASIL C 和 D 的安全目标。如果一个硬件元器件的诊断覆盖率（针对残余故障）低于 90%，应对其使用专用措施（9.4.2.4 中的注，列举了专用措施的示例）。

注：当确定安全机制的覆盖率时，可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。

9.4.2.6 此要求适用于等级为 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。

9.4.2.7 此要求适用于等级为 ASIL(B)、C 和 D 的安全目标。为了避免对量值有倾向性，如果从多个来源的失效率被组合，它们应按一个比例因子进行换算以保持一致。如果两个失效率来源间的比例因子存在根据，则换算是可行的。

注：附录 F 给出了应用比例因子的指导。

9.4.3 对违背安全目标的每个原因进行评估

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。

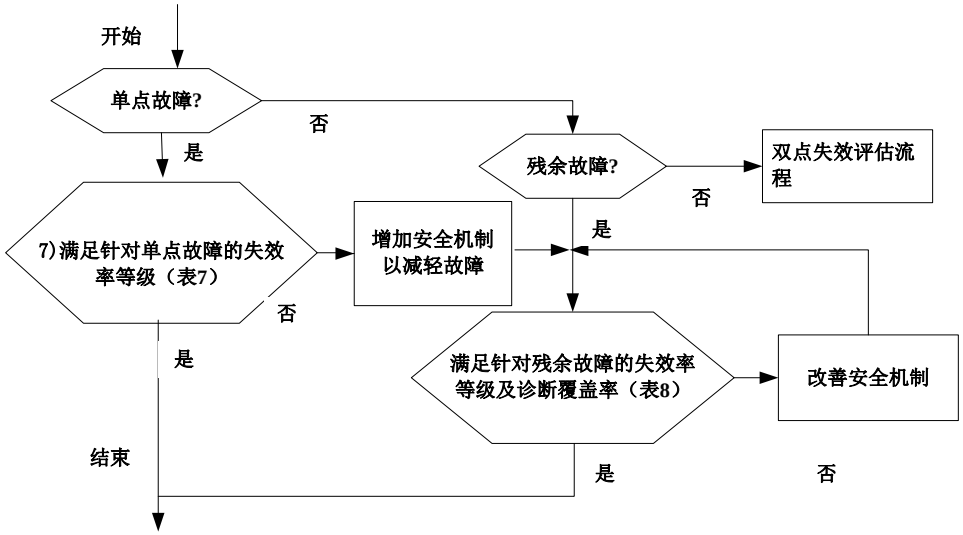


图 3 对单点和残余故障的评估流程

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。图 3 和 4 中描述的评估流程适用于硬件元器件（晶体管等）层面。

注：对于像微控制器这样复杂的硬件元器件，将此流程应用到更细节的层面，如 CPU、RAM、ROM 等，可能更恰当。

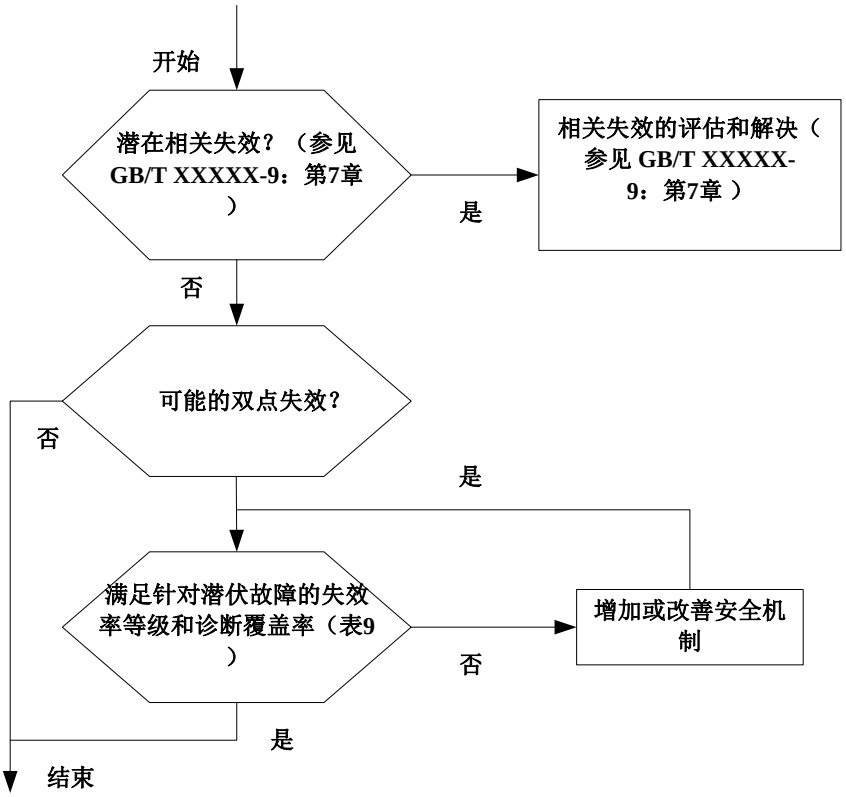


图 4 对双点故障的评估流程

9.4.3.2 此要求适用于等级为 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 9.4.3.12 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：此分析可被看作是对割集的评审，缺失或覆盖率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：对于像微控制器这样复杂的硬件元器件，将此流程应用到更细节的层面，如 CPU、RAM、ROM 等，可能更恰当。

9.4.3.3 此要求适用于等级为 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 的目标除以 100；除了应用 9.4.3.4；

注 2：可使用表 6 中给出的目标值。

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

c) 失效率等级 3 对应的失效率应少于或等于 100 倍的失效率等级 1 对应的失效率；
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：失效率等级的分配基于硬件元器件失效率。

注 4：对于元器件中的少数（如微控制器）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，则这些元器件可被分配等级 i。

9.4.3.4 如果给出理由说明失效率等级评级可除以一个小于 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：理由可基于最小割集的数量。

9.4.3.5 此要求适用于等级为 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 或 失效率等级 1
B	失效率等级 2 或 失效率等级 1
[a] 要求 9.4.2.4 的注给出了专用措施的示例。	

注：当评估失效率等级时，可考虑硬件元器件的安全故障比例。

9.4.3.6 此要求适用于等级为 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 中为相应的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，不包含安全机制的有效性。

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 9.4.2.4 的注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：当决定安全机制的覆盖率时，可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 此要求适用于等级为 ASIL C 和 D 的安全目标。对失效率等级 i，i＞3，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 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，可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 此要求适用于等级为 ASIL D 的安全目标。双点失效应被认为是可能的，如果：

a) 涉及到的一个或两个硬件元器件，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区间。

注：在确定安全机制的覆盖率时，可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 此要求适用于等级为 ASIL C 的安全目标。双点失效应被认为是可能的，如果：

a) 涉及到的一个或两个硬件元器件，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区间。

注：在确定安全机制的覆盖率时，可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 此要求适用于等级为 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 此要求适用于等级为 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，可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。

9.4.3.12 此要求适用于等级为 ASIL(B)、C 和 D 的安全目标。应使用 8.4.3 中描述的失效率来源对分析中用到的硬件元器件失效率的失效率等级评级进行证明。如果分析中用到了多个数据来源的失效率，那么应按照 9.4.2.7 描述的对失效率进行换算。

9.4.4 验证评审

此要求适用于等级为 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，以按照 GB/T XXXXX-8 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 9.4.2.4、9.4.2.5、9.4.3.5 和 9.4.3.6 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评审报告**，由 9.4.4 的要求得出。

10 硬件集成和测试

10.1 目的

本章的目的是通过测试确保所开发硬件符合硬件安全要求。

10.4.1至10.4.6的要求适用于要素的硬件。

10.2 总则

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

硬件集成和测试不同于GB/T XXXXX-8第13章中硬件组件鉴定活动，该活动为中等复杂性的硬件组件和元器件在符合GB/T XXXXX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：

— 安全计划（细化的），按照5.5；

— 相关项集成和测试计划（细化的），按照GB/T XXXXX-4中5.5.3；

— 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

可考虑下列信息：

— 项目计划（细化的）（参见GB/T XXXXX-4, 5.5.1）；及

— 硬件安全分析报告（参见7.5.2）。

10.4 要求和建议

10.4.1 硬件集成和测试活动应按照 GB/T XXXXX-8 第 9 章执行

10.4.2 硬件集成和测试活动应与 GB/T XXXXX-4,5.5.5 中给出的相关项集成和测试计划相协调。

注：如果已采用GB/TXXXXX-9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应采用分解前的ASIL等级。

10.4.3 测试设备应服从监控质量体系的控制

10.4.4 为了能适当定义所选硬件集成测试的测试案例，测试案例应使用表 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			
		A	B	C	D
1a	需求分析	++	++	++	++
1b	内部和外部接口分析	+	++	++	++
1c	等价类分析的生成[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、序列及来源分析	+	+	++	++
1h	环境条件和操作用例分析	+	++	++	++
1i	标准（如果存在）[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ISO 16750和ISO 11452。

[e]. 重要变量的分析包括最恶劣情况分析。

10.4.5 硬件集成和测试活动应当验证针对硬件安全要求的安全机制执行的完整性和正确性。

为了达到这些目的，应考虑表11所列方法。

表11 验证针对硬件安全要求的安全机制执行的完整性和正确性的硬件集成测试

方法		ASIL			
		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]. 功能测试的目标是验证相关项的具体特性已经达到。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]. 故障注入测试的目标是在硬件产品中引入故障并分析其响应。当定义了安全机制时，故障注入测试总是适用的。尤其是当硬件产品级的故障注入测试很难进行时，也可采用基于模型的故障注入(例如：在门级网表级注入故障)。例如，由于需要辐照试验，安全机制对硬件内部（微控制器）的瞬时故障的响应很难在硬件产品级进行故障注入来体现。

[c]. 电气测试的目标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。

10.4.6 硬件集成和测试活动应验证硬件在外部压力下的鲁棒性。

为了达到该目的，应考虑表12所列方法。

表12 验证在外部压力下的鲁棒性和运行的硬件集成测试

方法		ASIL			
		A	B	C	D
1a	环境测试带基本功能验证[a]	++	++	++	++
1b	扩展功能测试[b]	o	+	+	++
1c	统计测试[c]	o	o	+	++
1d	最坏情况测试[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]. 在环境测试带基本功能验证中，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]. 统计测试的目标是，根据实际的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标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。硬件的相关反应被检验并与特定要求比较。

[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。

[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]. 这些测试的目标是研究要素能经受的住的平均故障间隔期或者最大循环数。测试可以进行直到失效发生或者损毁评估时。

[i]. EMC测试，适用ISO 7637-2, ISO 7637-3, ISO 10605, ISO 11452-2 和 ISO 11452-4；ESD测试，适用ISO 16750-2。

[j]. 化学测试，适用ISO 16750-5。

10.5 工作成果

10.5.1 硬件集成和测试报告，由 10.4.1 至 10.4.6 要求得出。

附录A

（资料性附录）

产品开发硬件层面的概览和工作流

表A.1提供了产品开发硬件层面特定阶段的目的、前提条件和工作成果的概览。

表 A.1 产品开发硬件层面概览

条目	目的	前提条件	工作成果
5 启动硬件层面产品开发	启动硬件层面产品开发的目的是确定并计划系统各子阶段开发过程中的功能安全活动，也包括在GB/T XXXXX-8中所描述的必要的支持过程。 硬件特定的安全活动的计划包含在安全计划中。（参见GB/T XXXXX-2中6.4.3和GB/T XXXXX-4中5.4）。	项目计划（细化的）（按GB/T XXXXX-4，5.5.1） 安全计划（细化的）（按照GB/T XXXXX-4，5.5.2） 相关项集成和测试计划（细化的）（按照GB/T XXXXX-4，5.5.5）	5.5 安全计划（细化的）
6 定义硬件安全要求	本章的第一个目的是定义硬件安全要求，这些要求由技术安全概念和系统设计规范导出。本章的第一个目的是定义硬件安全要求，这些要求由技术安全概念和系统设计规范导出。 第二个目的是验证硬件安全要求与技术安全概念及系统设计规范的一致性。 本阶段另一目的是细化最初在GB/T XXXXX-4第7章定义的软硬件接口（HSI）规范。	安全计划（细化的）（按照 5.5 的要求） 技术安全概念（按照GB/T XXXXX-4，7.5.1） 系统设计规范(按照GB/T XXXXX-4，7.5.2） 软硬件接口规范(按照 GB/T XXXXX-4，7.5.3）	6.5.1 硬件安全需求规范（包括测试和认可准则） 6.5.2 软硬件接口规范（细化的） 6.5.3 硬件安全要求验证报告
7 硬件设计	本章的第一个目的是按照系统设计规范和硬件安全要求设计硬件。 本章的第二个目的是验证硬件设计是否违背系统设计规范和硬件安全要求。	硬件安全需求规范（按照 6.5.1） 硬件与软件接口规范（细化的）（按照6.5.2） 系统设计规范（按照GB/T XXXXX-4，7.5.2）	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。

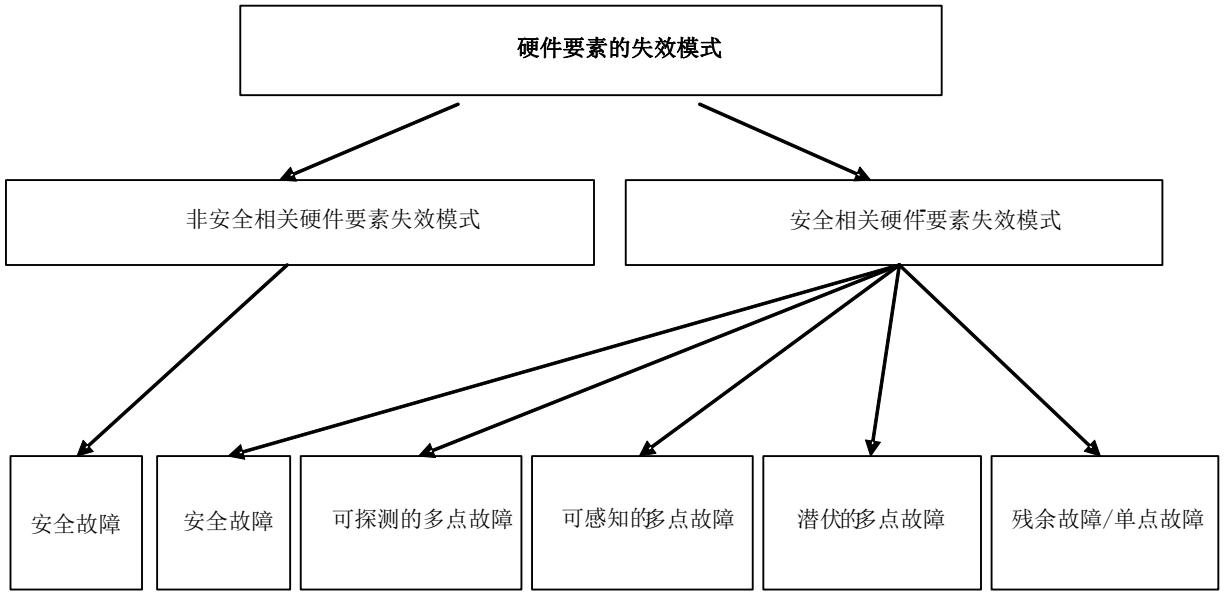
		安全计划（细化的）（按照5.5）	7.5.3 硬件设计验证报告，由 7.4.4 的要求得出。 7.5.4 与生产、运行、维护和报废相关的需求规范，由 7.4.5 的要求得出。
8. 硬件架构度量的评估	本章的目的是用表征故障处理要求的硬件架构度量来评估相关项的硬件架构。	硬件安全需求规范(按照6.5.1) 硬件设计规范(按照7.5.1) 硬件安全分析报告(按照7.5.2)	8.5.1 相关项架构应对随机硬件失效的有效性的分析 8.5.2 相关项架构应对随机硬件失效的有效性评估的评审报告
9 随机硬件失效导致违背安全目标的评估	本章中要求的目的是制定可用的准则，用于表明相关项随机硬件失效导致违背安全目标的残余风险足够低。	硬件安全需求规范(按照6.5.1) 硬件设计规范(按照7.5.1) 硬件安全分析报告(按照7.5.2)	9.5.1由随机硬件失效导致违背安全目标的分析 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 9.5.3 对随机硬件失效导致违背安全目标进行评估的评审报告
10 硬件集成和测试	本章的目的是通过测试确保所开发硬件符合硬件安全要求。 10.4.1 至 10.4.6 的要求适用于要素的硬件。	安全计划（细化的）(按照 5.5) 相关项集成和测试计划（细化的）(按照GB/T XXXXX-4中5.5.3) 硬件安全需求规范(按照 6.5.1) 硬件设计规范(按照7.5.1)	10.5 硬件集成和测试报告，由10.4.1至10.4.6要求得出。

附录B

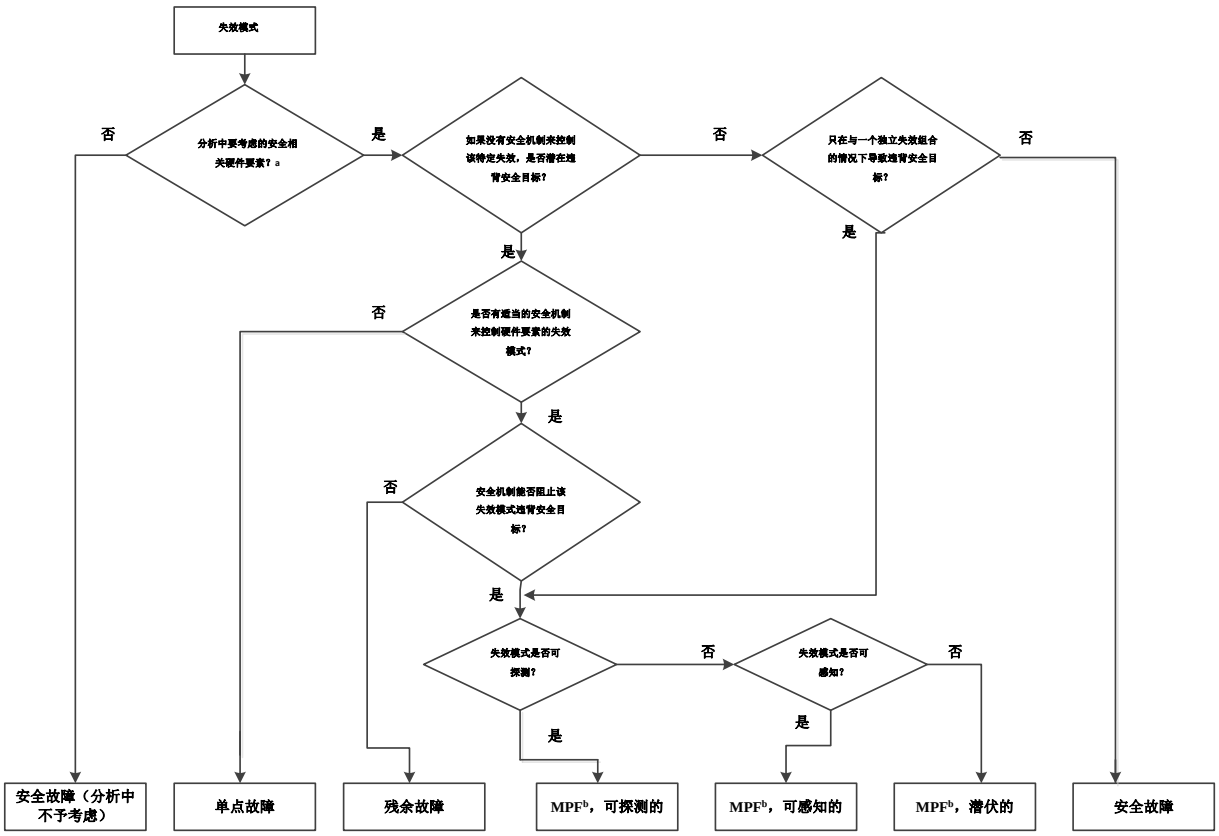
（资料性附录）

硬件要素的失效模式分类

硬件要素的失效模式可按图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



[a] 有些要素的失效不会显著增加违背安全目标的概率，可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，故障只导致$n>2$的多点失效的硬件要素，除非在技术安全概念中表明其是相关的。

[b] MPF表示多点故障.

注1：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。

注2：在考虑不同的安全目标时，同一故障可被归入不同的类别

图B.2 失效模式分类流程图示例

附录C

（规范性附录）

硬件架构度量

C.1故障分类和诊断覆盖率

C1.1 此要求适用于等级为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的违背安全目标的安全相关硬件要素。

示例： n>2的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。

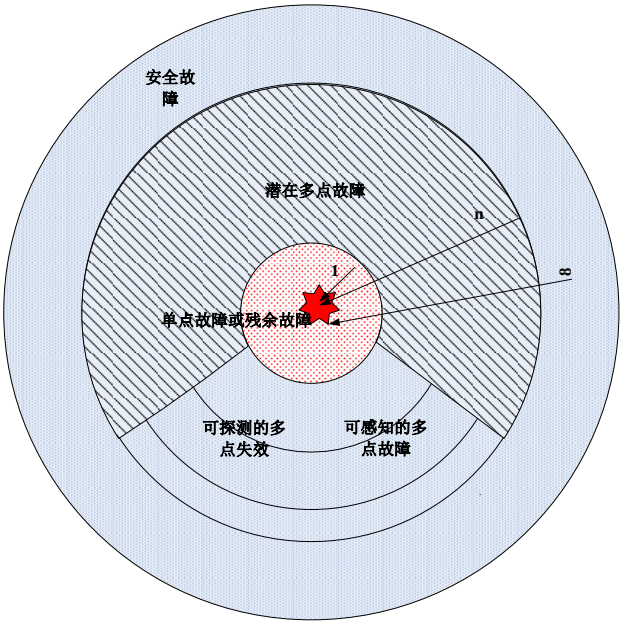
C1.2 此要求适用于等级为ASIL (B), C和D的安全目标。发生在安全相关硬件要素上的每个故障应按照图B.1中阐明的归类为：

a) 单点故障
b) 残余故障

示例：硬件要素可以有“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，那么它是一个残余故障。

c) 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的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

在这个图示中:

— 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；并且

— 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1：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，这样的故障可以被考虑为已探测出的多点故障，即使驾驶员从未被告知故障的存在。

示例： 在使用一个错误校正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，通过写回一个正确的值），相关项被修复为一个无故障状态。

因此每个安全相关的硬件要素的失效率λ都可按照等式(C.1)来表述（假设所有的失效都是互相独立的，且按照指数分布），如下：

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

其中

λ_{SPF} 是与硬件要素单点故障相关联的失效率

λ_{RF} 是与硬件要素残余故障相关联的失效率

λ_{MPF} 是与硬件要素多点故障相关联的失效率

λ_{S} 是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，□ MPF，可以按照等式(C.2)来表述，如下：

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

其中

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

$\lambda_{MPF,L}$ 是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可以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。

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

$$\lambda_{RF} \leq \lambda_{RF,est} = \lambda \times \left(1 - \frac{K_{DC,RF}}{100}\right)$$

其中

$\lambda_{RF,est}$ 是关于残余故障的估算的失效率

$K_{DC,RF}$是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可以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.4)提供了一个关于潜伏故障的失效率的保守估算。

$$K_{DC,MPF,L} = \left(1 - \frac{\lambda_{MPF,L,est}}{\lambda}\right) \times 100 \quad (C.4)$$

$$\lambda_{MPF,L} \leq \lambda_{MPF,L,est} = \lambda \times \left(1 - \frac{K_{DC,MPF,L}}{100}\right)$$

其中

$\lambda_{MPF,L,est}$是关于潜伏故障的估算的失效率.

$K_{DC,MPF,L}$是关于潜伏故障的诊断覆盖率，用百分比表示。

注2： 针对这个目的，附录D可作为声明的有合适理由支持的诊断覆盖率的基础。

注3： 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可以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 此要求适用于等级为ASIL (B)、C和D的安全目标。等式(C.5)中的计算应用于确定单点故障度量：

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

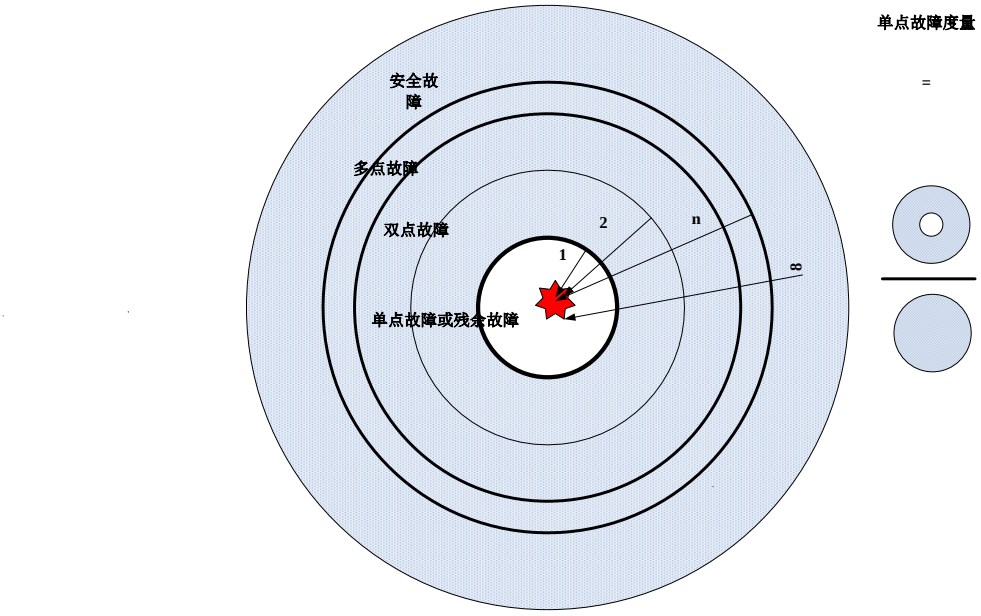
其中，$\sum_{SR,HW}(\lambda_X)$是在度量中考虑的相关项安全相关硬件要素的λ x总和。

注1： 该度量仅考虑明显的可能导致违背安全目标的相关项安全相关硬件要素。

示例：除非与技术安全概念相关，对于硬件要素的多点故障（n>2），可以在计算中被忽略。

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

$$1-\frac{\sum_{SR,HW}(\lambda_{MPF,\ latent})}{\sum_{SR,HW}(\lambda-\lambda_{SPF}-\lambda_{RF})}=\frac{\sum_{SR,HW}(\lambda_{MPF,\ perceived\ or\ detected}+\lambda_S)}{\sum_{SR,HW}(\lambda-\lambda_{SPF}-\lambda_{RF})} \quad (C.6)$$

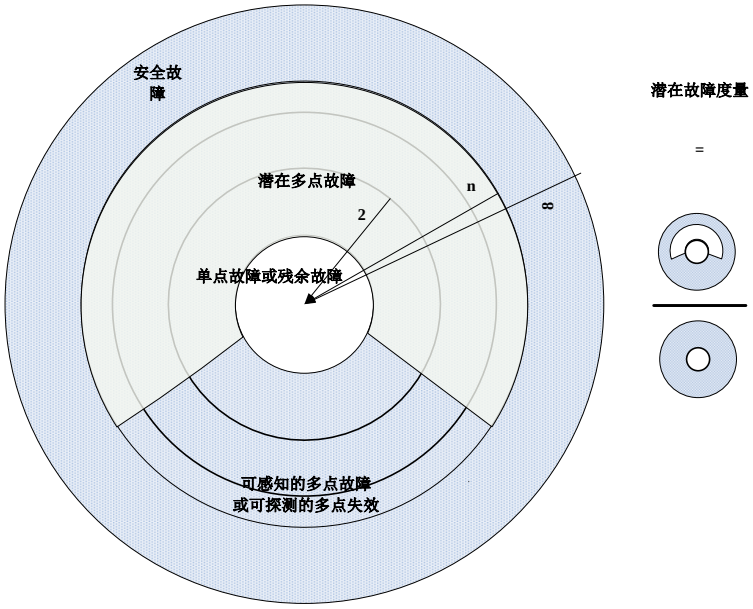
其中，$\sum_{SR,HW}\lambda_x$是在度量中考虑的相关项安全相关硬件要素的λ_x总和。

注1：该度量仅考虑明显的可能导致违背安全目标的相关项中安全相关硬件要素。

示例： 除非与技术安全概念相关，对于硬件要素的多点故障（n>2），可以在计算中被忽略。

注2： 图C.3给出了潜伏故障度量的图示。

注3: 附录E给出了计算“潜伏故障度量”的示例。



图C.2 潜在故障度量的图示

附录 D

（资料性附录）

诊断覆盖率的评估

D.1 总则

此附录的目的是用于：

a) 诊断覆盖率的评估，为以下提供理由：

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，这些安全机制在电子电气架构中探测要素的失效。

图D.1表示通常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故障或失效，同时包含了诊断覆盖率的指南。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故障。表中没有列举所有的故障，可以根据其它已知的故障或实际应用做调整。

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.14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故障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定义为60%、90%或99%的典型覆盖水平。

对故障及其相应的安全机制的诊断覆盖等级的指定，根据下列条件可与表D.1中不同：

c） 被诊断探测到的故障类型来源的不同；

d） 安全机制的有效性；

e） 安全机制的特定实现；

f） 安全机制（周期性）的执行时序；

g） 在系统中使用的硬件技术；

h） 基于系统中硬件的失效模式的概率；

i） 对故障及其分成不同诊断覆盖率水平的几个子集的更详细分析。

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.1到D.14可以被视为一个起点，可以被用来作为评估这些有恰当理由支持的安全机制的诊断覆盖率。另外，所给信息是用来帮助定义要素故障或失效模式；然而，相关的失效模式最终依赖于要素应用场合。

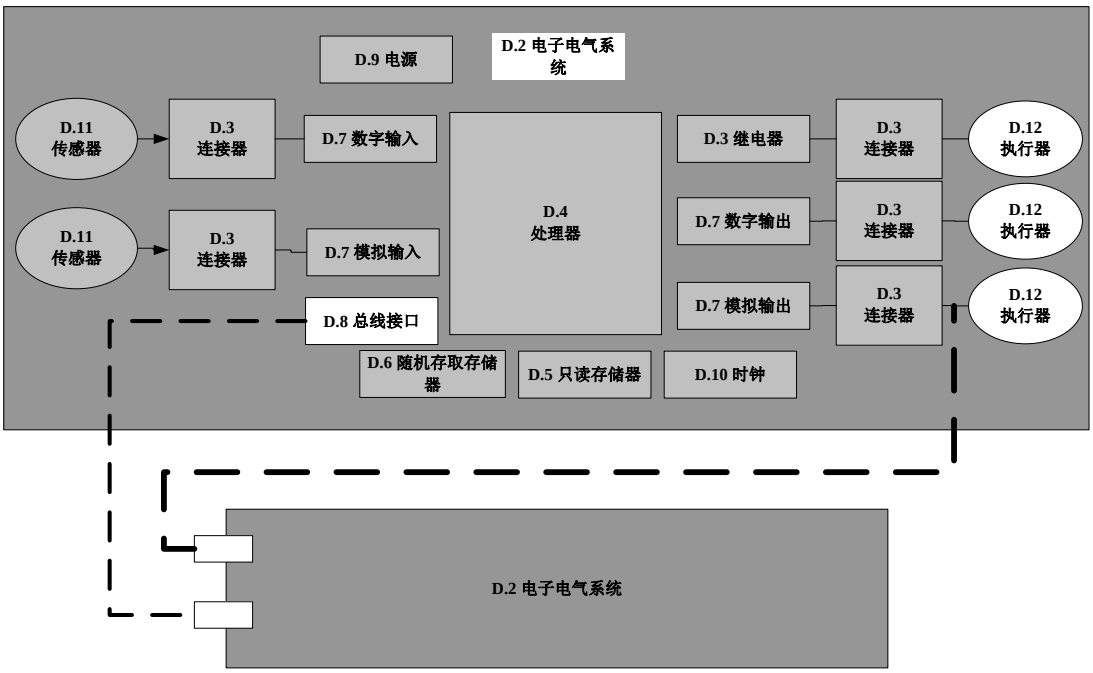


图 D.1 常见系统硬件

通过给出诊断测试技术的指导准则，表D.2到D.14支持表D.1的信息。D.1到D.14并不完备，只要有证据支持声明的诊断覆盖率，也可以采用其它技术。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 源于诊断覆盖率的、所需分析的故障或失效模式

要素	参考表格	60%、90%、99%诊断覆盖率对应的、所需分析的失效模式		
		低(60%)	中(90%)	高(99%)
总体要素				
电子电气系统	D.2	无通用的故障模型。 必要的细节分析。	无通用的故障模型。 必要的细节分析。	无通用的故障模型。 必要的细节分析。
电气要素				

继电器	D.3	不通电或不断电。 触点熔接。	不通电或不断电。 单个触点熔接。	不通电或不断电。 单个触点熔接。
线束，含接头和连接器		开路。 短接到地。	开路。 短接到地。(直流耦合) 短接到电源。 相邻插针间短接。	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。 插针间电阻漂移。
传感器，含信号开关	D.11	无通用的故障模型。 必要的细节分析。 应覆盖的典型的失效模式包括： 超出范围 在范围之内卡滞 (陷入，停留在)(后两列同)	无通用的故障模型。 必要的细节分析。 应覆盖的典型的失效模式包括： 超出范围 偏移 在范围之内卡滞（卡滞）	无通用的故障模型。 必要的细节分析。 应覆盖的典型的失效模式包括： 超出范围 偏移 在范围之内卡滞（卡滞） 振荡
终端要素(执行器，灯，蜂鸣器，显示屏等等)	D.12	无通用的故障模型。 需要细节分析。	无通用的故障模型。 需要细节分析。	无通用的故障模型。 需要细节分析。
常规半导体要素				

电源	D.9	过压或欠压	漂移 过压或欠压	漂移和振荡 过压或欠压 电源毛刺
时钟	D.10	卡滞故障[a]	直流故障模型[b]	直流故障模型[b] 频率错误 周期抖动
非易失性存储器	D.5	数据，地址，控制接口，控制线和控制逻辑的卡滞故障[a]	数据，地址（包括同一存储块内的地址线），控制接口，控制线和控制逻辑的直流故障模型[b]	数据，地址（包括同一存储块内的地址线），控制接口，控制线和控制逻辑的直流故障模型[b]
易失性存储器	D.6	卡滞故障[a]（包括微控制器外部的信号线）	数据，地址（包括同一存储块内的地址线），控制接口，控制线和控制逻辑的直流故障模型[b] 位存储单元软错误模型	数据，地址（包括同一存储块内的地址线），控制接口，控制线和控制逻辑的直流故障模型[b] 位存储单元软错误模型[c]
数字输入/输出 模拟输入/输出	D.7	卡滞故障[a]（包括微控制器外部的信号线）	直流故障模型[b]（包括微控制器外部的信号线）	直流故障模型[b]（包括微控制器外部的信号线） 漂移和振荡
特殊半导体要素				

处理单元	算数和逻辑单元（ALU）的数据路径	D.4/D.13	卡滞故障[a]	门级卡滞故障[a]	直流故障模型[b] 软错误模型（针对序列元器件）
	寄存器(通用寄存器堆， DMA 转换寄存器)，内部 RAM	D.4	卡滞故障[a]	门级卡滞故障[a] 软错误模型[c]	直流故障模型[b]，包括寄存器无寻址、错误寻址、或者多个寻址 软错误模型[c]
	地址运算(负载/存储单元,DMA 寻址逻辑，存储器和总线接口)	D.4/D.5/D.6	卡滞故障[a]	门级卡滞故障 软错误模型[c]（针对序列的元器件）	直流故障模型[b]，包括寄存器无地址、错误地址或者多地址 软错误模型[c]（针对序列的元器件）
	中断处理	D.4/D.10	遗漏或者连续的中断	遗漏或者连续的中断 执行了错误的中断	遗漏或者连续的中断 执行了错误的中断 错误的优先级 缓慢或干扰中断处理导致丢失或延误的中断服务

	控制逻辑(顺序器、编码以及包含标志寄存器和堆栈控制的执行逻辑)	D.4/D.10	没有执行编码 执行过慢 堆栈上溢出/下溢出	编码错误或者没有执行 执行过慢 堆栈上溢出/下溢出	编码错误，执行错误或者没有执行 无序执行 执行过快或者过慢 堆栈上溢出/下溢出
	配置寄存器	D.4	—	卡滞至错误值	寄存器损坏（软错误） 卡滞故障模型
	其他不属于之前类别的一些子要素	D.4/D.13	卡滞故障[a]	门级卡滞故障	直流故障模型[b] 软错误模型[c]（针对序列的元器件）
通信	片上通信，含总线仲裁	D.14	卡滞故障[a]（数据控制，地址和仲裁信号）	直流故障模型[b]（数据控制，地址和仲裁信号)超时 没有或者持续不断的仲裁	直流故障模型[b]（数据控制，地址和仲裁信号） 超时 没有或者持续不断或者错误的仲裁 软错误（针对序列的元器件）

	数据传输(用 GB/TXXXX-6 附录 D 来进行分析)	D.8	通信节点失效 消息损坏 消息延迟 消息丢失 非预期消息重复	之前项 + 顺序错误 消息插入	之前项 + 伪消息

注 1：基于分析，可以声明具有更高的诊断覆盖率。 同样地，如果主要的失效模式没有被列出来，那么就会导致更低诊断覆盖率。

注 2：当显示与所使用的技术相关时，瞬态故障需要被考虑。

注 3：可对处理单元的失效模式进行调整以识别交流故障模型，比如转换故障(在应用频率节点缓慢上升，缓慢下降)和路径延迟。这种类型的故障在更小尺寸工艺中越来越普遍。由于这些类型的故障的测试具有侵入性本质且具有通过容限测试能较早探测出失效的能力，对其进行的测试通常是在启动或下电、或两者过程中完成的。因为难以定量，所以这些失效模式通常不包含在失效率的计算中。

注 4：如果应用恰当，由卡滞故障模拟得到的方法(比如 N 型探测测试)，在应用条件下执行，对于直流故障模型以及转换模型同样有效。

[a] 卡滞是一个故障类型，可以描述为要素针脚上持续的“0”、“1”或者 “打开”。该故障只针对具有要素层针脚接口的要素才是有效的。

[b] 直流故障模型（“直接电流故障模型”）包含下列失效模式：卡滞故障，卡滞开路，开路或者高阻抗输出，以及信号线间的短路。这里的意图不是一定需要全面的分析，比如要求对于微控制器内或者来自于一个复杂的 PCB 板上任何理论可能的信号组合的桥接故障进行详尽的分析。分析着重于主要信号或者在布局层面分析中识别出的高度耦合互连。

[c] “软错误模型”：软错误（比如位翻转）是由封装衰变的 α 粒子或者中子等引起的瞬态故障的结果。这些瞬态故障也就是信号状态翻转（SEU）和信号状态突变（SET）。

表 D.2 系统

安全机制/措施	参见技术概览	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
模拟信号监控优先于数字开/关状态监控	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	参见技术概览	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：该表格仅涉及用于电器要素的安全机制。通用技术，如基于数据的比较（参见 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 中）

表 D.4 处理单元

安全机制/措施	参见技术概览	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：该表格仅涉及用于处理单元的安全机制。通用技术，如基于数据的比较（参见表格 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 中）			

表 D.5 非易失性存储器

安全机制/措施	参见技术概览	可实现的典型诊断覆盖率	备注
校验位	D.2.5.2	低	—
使用错误探测纠错码(EDC)监控内存	D.2.4.1	高	有效性取决于冗余的比特数。可以用来纠错

改进的校验和	D.2.4.2	低	取决于在测试区域内的错误位的数量和位置
储存器特征码	D.2.4.3	高	—
存储块复制	D.2.4.4	高	—

表 D.6 易失性存储器

安全机制/措施	参见技术概览	可实现的典型诊断覆盖率	备注
RAM 模式测试	D.2.5.1	中	对卡滞失效具有高覆盖率。对链接失效没有覆盖。适合在中断保护下运行
RAM 跨步测试	D.2.5.3	高	对链接单元的覆盖率取决于写和读的次序。测试通常不适合在运行时进行。
校验位	D.2.5.2	低	—
使用错误探测纠错码的内存监控（EDC）	D.2.4.1	高	有效性取决于冗余的比特数。可用于纠错

存储块复制	D.2.4.4	高	共因失效模式会降低诊断覆盖率
运行校验和/CRC	D.2.5.4	高	特征码的有效性取决于一个与被保护的存储块长度有关的多项式。 应当注意在校验和计算期间，用于确定校验和的值不能被改变。 如果返回的是随机数据模式，那么可能性就是校验和最大值的倒数

表 D.7 数字和模拟输入/输出

安全机制/措施	参见技术概览	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.2.6.1	高	取决于模式类型
数字输入/输出的编码保护	D.2.6.2	中	取决于编码类型
多通道并行输出	D.2.6.3	高	—

受监控的输出	D.2.6.4	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.2.6.5	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.8 通信总线（串行，并行）

安全机制/措施	参见技术概览	可实现的典型诊断覆盖率	备注
一位硬件冗余	D.2.7.1	低	—
多位硬件冗余	D.2.7.2	中	—
发送的消息回读	D.2.7.9	中	—
完全硬件冗余	D.2.7.3	高	共模失效模式会降低诊断覆盖率
使用测试模式检验	D.2.7.4	高	—
发送冗余	D.2.7.5	中	取决于冗余类型，只对瞬态故障有效

信息冗余	D.2.7.6	中	取决于冗余类型
帧计数器	D.2.7.7	中	—
超时监控	D.2.7.8	中	—
信息冗余，帧计数器和超时监控的组合	D.2.7.6, D.2.7.7 and D.2.7.8	高	对于没有硬件冗余和测试模式的系统，这些安全机制的综合可以声明达到高覆盖率

表 D.9 电源

安全机制/措施	参见技术概览	可实现的典型诊断覆盖率	备注
电压或电流控制（输入）	D.2.8.1	低	—
电压或者电流控制（输出）	D.2.8.2	高	—

表 D.10 程序序列监控/时钟

安全机制/措施	参见技术概览	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.2.9.1	低	—
具有独立时间基准和时间窗口的看门狗	D.2.9.2	中	取决于时间窗口的时间限制
程序序列的逻辑监控	D.2.9.3	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.2.9.4	高	—
基于时间的程序序列的时间和逻辑联合监控	D.2.9.5	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次序的覆盖。 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.11 传感器

安全机制/措施	参见技术概览	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.2.6.1	高	—
输入比对/表决（1oo2, 2oo3 或者更好的冗余）	D.2.6.5	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.2.10.1	低	探测对地或电源短路，和部分开路
传感器相关性	D.2.10.2	高	探测有效范围内失效
传感器合理性检查	D.2.10.3	中	—

表 D.12 执行器

安全机制/措施	参见技术概览	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.2.6.1	高	—
监控(即一致性控制)	D.2.11.1	高	取决于失效探测的诊断覆盖率

表 D.13 组合和顺序逻辑

安全机制/措施	参见技术概览	可达到的典型诊断覆盖率 (直流失效模型)	备注
通过软件实现的自检	D.2.3.1	中	--
硬件支持的自检（单通道）	D.2.3.2	高	有效性取决于自检的类型.门级是此测试的适当级别

表格 D.14 片上通信

安全机制/措施	参见技术概览	可达到的典型诊断覆盖率	备注
单位硬件冗余	D.2.7.1	低	--
多位硬件冗余	D.2.7.2	中	多位冗余通过适当的数据，地址和控制线的交错，而且如果与一些完全冗余相结合（例如，提供给仲裁），可以达到高的诊断覆盖率。
全硬件冗余	D.2.7.3	高	共因失效模式可以降低诊断覆盖率

测试模式	D.2.6.1	高	取决于模式类型
注：此表提供了微处理器内部通信总线的覆盖率。			

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.7、D.11和D.12引用了此技术/措施。

目标：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刻却没有改变状态，就可以被探测为一个失效。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 时此参数翻转，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

目标：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：通过比较器连续的或周期性的比较独立硬件的输出信号或独立软件的输出信息。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。

目标：探测和屏蔽 3 个以上通道中有 1 个发生的失效。

描述：表决单元使用多数原则（3 个中的 2 个，3 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

目标：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 模拟信号监控优先于数字开/关状态

注：表 D.2 引用了此技术/措施。

目标：提升测量信号的可信性。

描述：只要有选择，模拟信号的使用都优先于数字开/关状态。例如，用模拟信号水平表征错误或者安全状态，并常伴有信号水平偏差监控。对于数字信号，也有可能通过模拟输入来监控。此技术对发射器进行持续的监控，使其具有更高的可信度，同时也降低了对发射器感应功能失效进行周期性探测所需的频率。

D.2.3 处理单元

整体目标：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 和 D.13 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它具有物理存储（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 和 D.13 引用了此技术/措施。

目标：使用提高失效探测速度和扩展失效探测范围的专用硬件，尽早探测出处理单元和其它子要素中的失效。

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它子要素（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，此测试仅典型的在处理单元初始化或者下电时运行，并典型的用于多点故障探测。

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。

目标：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：失效探测完全通过两个或更多处理单元各自执行附加软件功能来进行自检（例如走位模式）以探测物理存储（数据和地址寄存器）和功能单元（例如，指令解码器）可完全实现此失效探测。然后处理单元间交换结果。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。

目标：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。.

一个实现方式，作为主路径，负责计算，如果计算错误可导致一个危害。另一个实现方式，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（参见图 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(参见参考文献[21])。

另一种版本的安全机制是通过对主路径进行原样的复制（或者是将主路径执行两次）来实现冗余路径。这种版本中没有软件冗余，只能够覆盖软错误。如果进行第三次代码的执行，将已知输入产生的输出与预期输出相比较，可达到中等覆盖率。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）和实现方法（无需设计冗余路径），但是此概念包含了对历史项的保存（如动态状态、积分电路、变化速度限制等）。

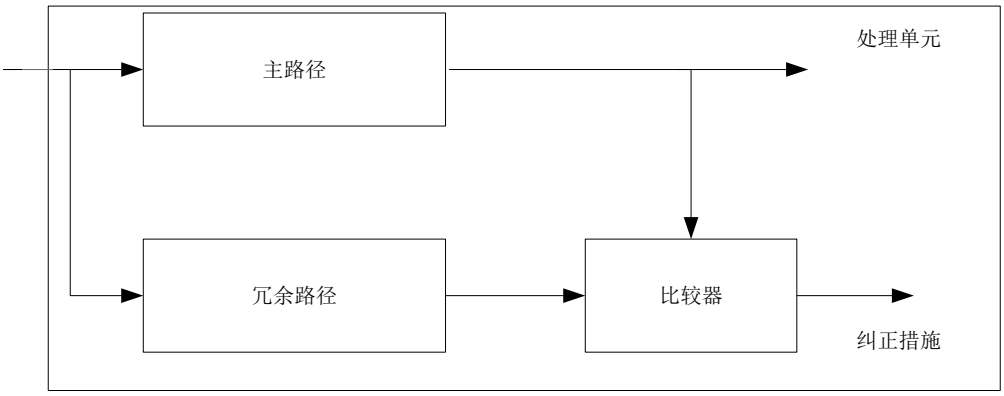


图 D.2 相同处理单元中的冗余软件比较

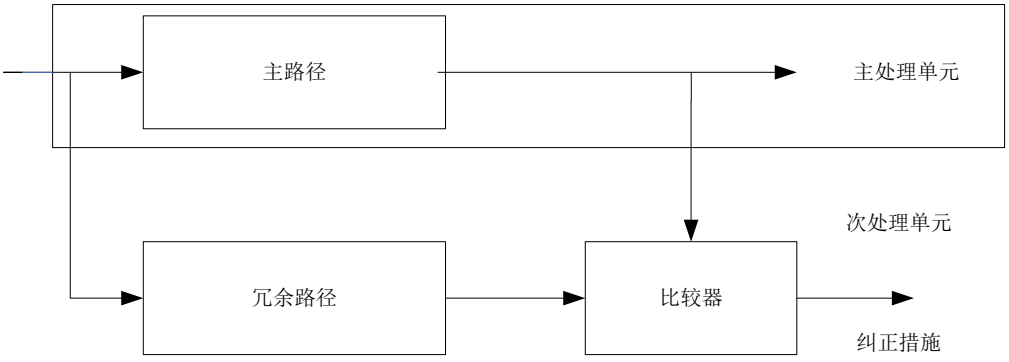
D.2.3.5 分立处理单元中的软件进行相互比较

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（参见图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)而产生的不正确的错误探测的方法。

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

D.2.3.6 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（参见参考文献[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。

其它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。此方法的缺点是可能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。可能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 非易失性存储器

整体目标：探测非易失性存储器中的信息损坏。

注：基于应用的存储器类型，一个单点故障可能会影响多个存储位置。例如，行选择线开路将阻止读取存储器的一整行。如果测试多个存储位置，此类失效会很容易被探测出来。

D.2.4.1 使用错误探测校验码监控存储器（EDC）

注1：表D.5和D.6引用了此技术/措施。

目的：探测每个字（典型的为32、64或128位）中每个单位失效、每个双位失效、某些三位失效以及某些全位失效。

描述：把存储器的每个字扩展几个冗余位从而生成汉明距离至少为4的、修改的汉明码。每次读字时，通过检查冗余位可确定是否发生破坏。当发现差异时，就生成失效信息。

此流程也能够通过计算数据字及其地址之间的关联的冗余位，而用于探测寻址失效。否则，对于寻址失效，探测的可能性将取决于返回的随机数的EDC位的个数（例如，地址线开路，或地址线与另一条地址线短路返回两个单元的平均值）。如果寻址错误导致选择了完全不同的单元，则覆盖率为0%。

对于RAM单元写使能失效，如果该单元不能被初始化，EDC能够提供高的覆盖率。如果写使能失效在初始化之后影响到整个单元，则覆盖率为0%。

注2：这种技术通常被称为ECC（纠错码）。

D.2.4.2 改进的校验和

注：表D.5引用了此技术/措施。

目的：探测每个单位失效。

描述：使用合适的算法生成校验和，此算法使用了存储器块中的每个字。校验和可作为额外字存储在ROM中，或者作为额外字写到存储块中，以保证校验和算法生成预定的值。在后面的存储器测试中，再使用同一算法生成一次校验和，并把该结果同存储的或者定义的值进行对比。如果发现有差异，则生成失效信息（参见参考文献[20]）。该技术对返回随机结果的漏探测概率是$1/(2^{校验和的长度})$，但某些校验和对有较大可能的特定数据干扰，能提供比随机结果更好的探测率。

D.2.4.3 存储器特征码

注1：表D.5引用了此技术/措施。

目的：探测每个一位失效和大部分的多位失效。

描述：使用例如循环冗余检验（CRC）算法，将存储块的内容压缩成（既可使用硬件也可使用软件）一个或多个字节。典型的CRC算法是把存储块的整个内容当作字节串或者位串

数据流来处理，使用多项式生成器对其执行连续的多项式除法。除的余数代表压缩的存储内容---这就是存储器的“特征码”，并被存储起来。在后面的测试中重新计算一次特征码，并将其与之前存储的特征码进行比较。当有差异时，就生成失效消息。

CRC对于探测区间错误特别有效。特征码的有效性取决于多项式，该式与受保护信息块的长度有关。如果返回随机结果，则漏探测的概率是1/（$2^{校验和的长度}$）（参见参考文献[20]）。

注2：基于当前技术，针对超过4k的存储器通常不考虑使用8位CRC。

D.2.4.4 存储块复制（例如，利用硬件或软件进行比较的双存储器）

注：表D.5和D.6引用了此技术/措施。

目的：探测每个位失效。

描述：在两个存储器中复制地址空间。第一个存储器以正常方式工作。第二个存储器包含同样的信息并且同第一个并行存取。比较它们的输出，当探测到有差异时就生成失效信息。取决于存储器子系统的设计，在两个存储器中的一个存储相反的数据能够提高诊断覆盖率。如果在两个存储块中存在共同的失效模式（例如共同的地址线、共同的写入准许）或存储单元的物理位置使逻辑上远离的单元却物理相邻，那么诊断覆盖率会被降低。

D.2.5 易失性存储器

整体目标：在寻址、写入、存储和读取的过程中探测失效。

注：基于应用的存储器类型，一个单一故障可影响到多个存储位置。例如，行选择线的开路会阻止存储器一整行的读取。如果测试多个存储位置，则更容易探测出此类故障。

D.2.5.1 RAM 模式测试

注1：表D.6引用了此技术/措施。

目的：探测主要的静态位失效。

描述：将位模式及其补码写入存储器的单元。

RAM位置通常被单独测试。单元内容被保存后，将全部单元写入0，然后通过回读所有的0值来验证单元内容。此过程将被重复为全部单元写入1并回读内容。如果从1到0的转换失效是所考虑的失效模式，可再执行一次写入和读取0的过程。最后，存入单元的初始值（见参考文献[20]，4.2.1条）。此测试对于探测卡滞失效和转换失效是有效的，但不能探测绝大多数的软错误、寻址故障和链接单元故障。

注2：在每个独立位置的测试过程中，此测试经常在中断禁止的情况下进行。

注3：因为测试的执行包括读取刚刚写入的值，优化编译器倾向于删除该测试。如果仍采用优化编译器，好的设计实践是通过汇编级代码检查来验证此测试代码。

注4：一些RAM可能发生失效以致对上一个存储单元的访问操作值返回作为当前单元的读取值。若这是一种可能的失效模式，诊断可同时测试这两个位置，首先对第一个位置写入一个0代替原来的1，随后对第二个位置写入一个1，然后验证从第一个位置读取的是否为0。

D.2.5.2 奇偶校验位

注：表D.5和D.6引用了此技术/措施。

目的：探测字中（典型的有8位、16位、32位、64位或128位）单个位或奇数个位失效。

描述：把存储器的每个字都扩展1位（奇偶校验位），此位给每个字补齐偶数个或奇数个逻辑“1”。每次读字时都将检查它的数据奇偶性。如发现1的个数有误，则生成失效信息。应这样选择偶校验或奇校验，即“0字”（全0）或“1字”（全1）中的哪一个在失效事件中更不期望发生，则不选择那个字码。

当计算数据字位和它的地址连接的奇偶性时，奇偶校验也可用来探测寻址失效。否则，对于寻址失效，对随机返回的数据的探测存在50%的概率（例如，地址线开路或地址线和其他地址线短路，返回两个单元的平均值）。如果地址错误导致完全选择不同的单元，覆盖率为0%。

对于RAM单元读取使能失效，如果该单元不能被初始化，奇偶校验能够探测50%的失效。如果读取使能失效在初始化之后影响到整个单元，覆盖率为0%。

D.2.5.3 RAM 跨步测试

注：表D.6中引用了此技术/措施。

目的：探测主要的持续位失效。位转换失效，寻址失效和链接单元失效。

描述：把一个0s和1s模式以特殊模式写入存储器单元中，并以特殊顺序加以验证。

当跨步要素是在处理另一个单元之前应用于存储阵列中每一个单元的一个有限操作序列，跨步测试由跨步要素的有限序列构成。例如，一个操作可能是写一个0到一个单元中，写一个1到一个单元中，从单元中读取预期的0，从单元中读取预期的1。如果预期的“1”没有被读出，失效就会被探测出来。对链接单元的覆盖程度取决于写/读的顺序。

参考文献[20]，第4章，列出了许多不同的跨步测试设计以探测不同的RAM失效模式：卡滞故障、转换故障（不能从1转换到0或从0转换到1但不包括两者都发生）、地址故障和链接单元故障。这些类型的测试对于软错误的探测无效。

注2：这些测试通常在初始化或关机时运行。

D.2.5.4 运行校验和/CRC

注：表D.6中引用了此技术/措施。

目的：探测RAM中的单位失效和某些多位失效。

描述：借助合适的算法来创立校验和，此算法使用了存储器块中的每个字位。校验和可作为附加字位存储在RAM中。由于存储块更新时，RAM校验和/CRC通过移除就数据值并在存储区域加入新数据值也会被加以更新。校验和/CRC为数据块周期性地进行计算并与存储的校验和/CRC进行对比。如果发现有差异，就产生失效信息。如果返回一个随机结果，则误探测的概率为1/校验和的长度或1/CRC的长度。诊断覆盖率可能会随存储器的增大而降低。

D.2.6 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.2.6.1 测试模式

注：表D.7、D.11、D.12和D.14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.2.6.2 编码保护

注：表D.7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：此流程保护输入/输出信息免受系统失效和随机硬件失效。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.2.6.3 多通道并行输出

注：表 D.7 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.2.6.4 受监控的输出

注：表 D.7 引用了此技术/方法。

目的：用于探测由外部影响导致的独立失效、时序失效、寻址失效、漂移失效(对于模拟信号)和瞬时失效。

描述：这是一个依赖于数据流的、具有独立输入以确保符合预先定义的公差范围(时间、值)的输出比较。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. 2.6.5 输入比较/表决

注：表 D.7 和表 D.11 引用了此技术/方法。

目的：用于探测由外部影响导致的独立失效、时序失效、寻址失效、漂移失效(对于模拟信号)和瞬时失效。

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. 2.7 通信总线

整体目标：探测信息传递的失效。

D. 2.7.1 一位硬件冗余

注：表 D.8 和表 D.14 引用了此技术/方法。

目的：用于探测每一个奇数位失效，即 50%数据流中所有可能的位失效。

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。

D2.7.2 多位硬件冗余

注：表 D.8 和表 D.14 引用了此技术/方法。

目的：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汉明(纠错)码技术来探测失效。

D. 2.7.3 完整硬件冗余

注：表 D.8 和表 D.14 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.2.7.4 使用测试模式检验

注：表 D.8 参考了此技术/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.2.7.5 发送冗余

注：表 D.8 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.2.7.6 信息冗余

注 1：表 D.8 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 可以包含在校验和/CRC 计算中，以提供对此部分信息的损坏覆盖(信息伪装)。

a) 低诊断覆盖率：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) 中等诊断覆盖率：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 位的数据，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，如果有适当的理由，仍能声明对数据和ID损坏达到高覆盖率。

D.2.7.7 帧计数器

注：表 D.8 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。

D2.7.8 超时监控

注：表 D.8 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.2.7.9 发送信息回读

注 1：表 D.8 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。其它的失效模式，如非预期的消息重复，是不一定被此安全机制覆盖到的。

D.2.8 电源

整体目标：探测电源缺陷导致的失效。

D.2.8.1 电压或电流控制(输入)

注：表D.9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.2.8.2 电压或电流控制(输出)

注：表 D.9 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.2.9 程序序列的时间和逻辑监控

注：表 D.10 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)运行在错误的顺序或时段，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.2.9.1 具有独立时间基准，无时间窗口的看门狗

注：表 D.10 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.2.9.2 具有独立时间基准和时间窗口的看门狗

注：表 D.10 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.2.9.3 程序序列的逻辑性监控

注：表 D.10 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.2.9.4 程序序列的时间和逻辑的联合监控

注：表 D.10 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 D2.9.3 与 D.2.9.1（或 D.2.9.2）的技术组合。

D.2.9.5 基于时间的程序序列的时间和逻辑联合监控

注：表 D.10 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.2.10 传感器

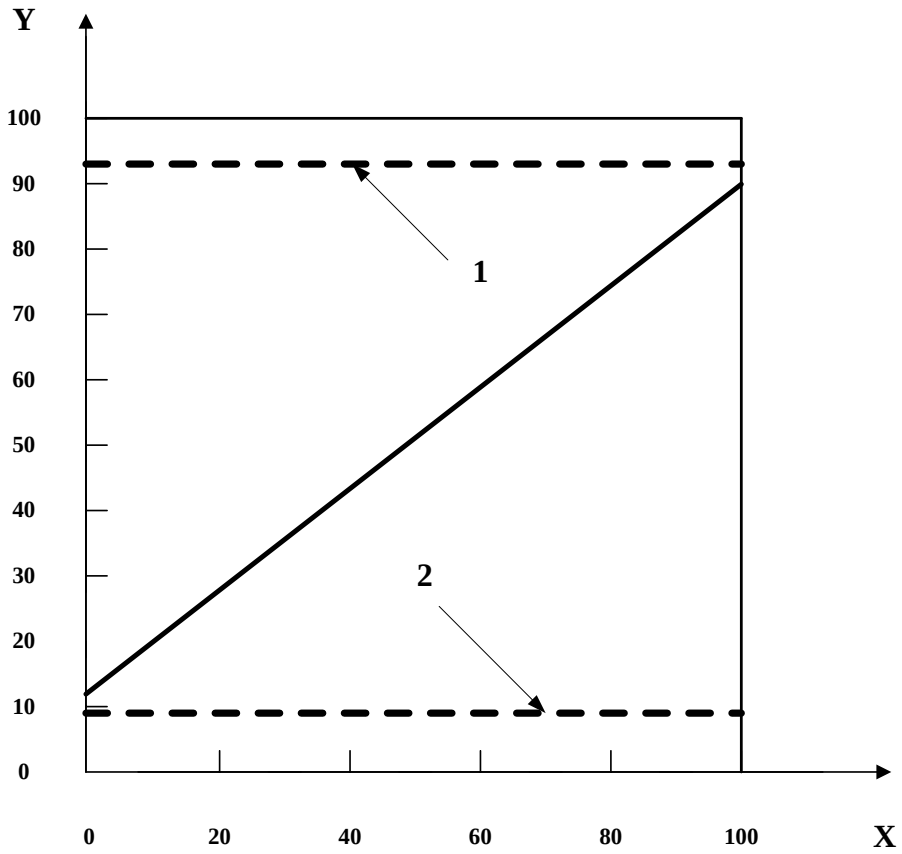
整体目标：控制系统的传感器失效。

D.2.10.1 传感器的有效范围

注：表 D.11 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，参见图 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。



略语表

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 传感器带有超量程区域

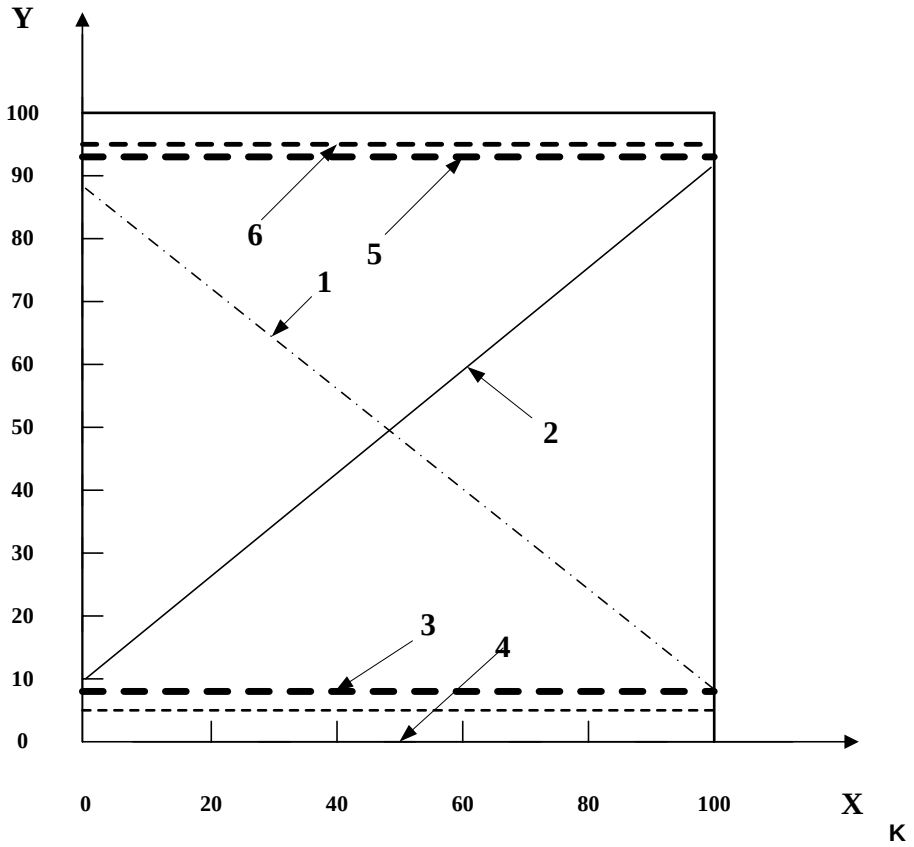
D.2.10.2 传感器相关性

注：表 D.11 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、偏移或其它错误。

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，参见图 D.5，两个斜率相同但方向相反的传感器。注，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，并在一个阀值范围内比较。选定阀值时需考虑 ADC 公差范围和电气元件的散差。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。



略语表

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

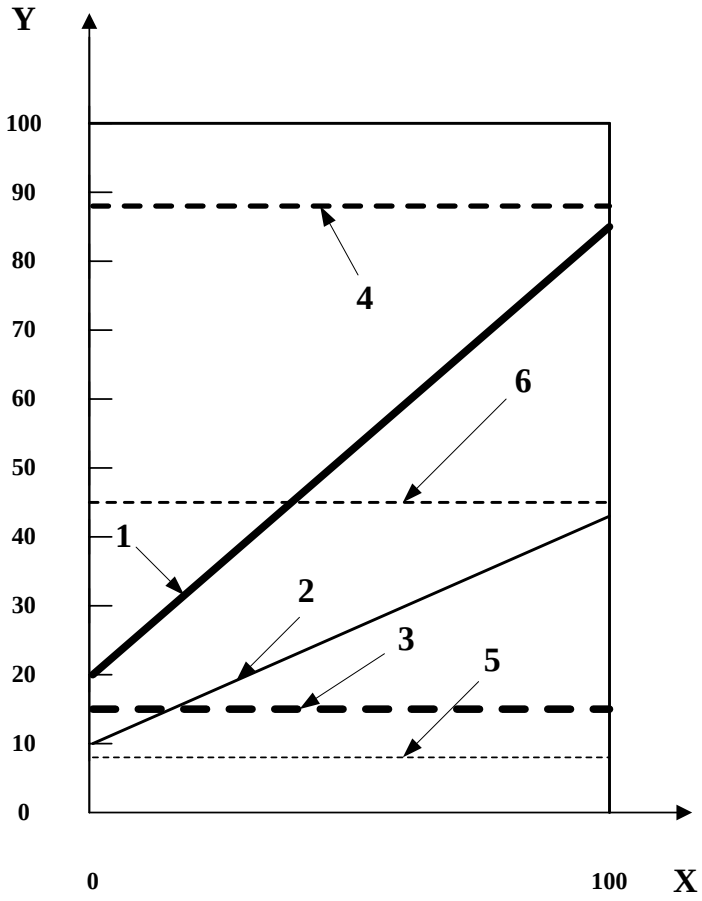
5 传感器1的超量程高门限

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传感器带有超量程区域

基于相等斜率的传感器，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，使两个传感器以相似方式损

坏。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。



略语表

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 一个传感器斜率是另一个一半的传感器带有超量程区域

D.2.10.3 传感器合理性检查

注：表D.11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、偏移或其它错误。

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.2.11 执行器

整体目标：控制系统终端要素的失效。

D.2.11.1 监控

注1：表D.12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。物理参数的监控依靠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

（资料性附录）

硬件架构度量计算范例：“单点故障度量”和“潜伏故障度量”

本附录给出了8.4.7和8.4.8中选项a)所要求的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的示例。

本示例中的系统在一个ECU中实现了两个功能。

功能1有一个输入（通过传感器R3测量温度）和一个输出（通过I71控制阀2），功能1的表现是当温度高于90°C时打开阀2。

如果没有电流经过 l71，阀 2 打开。

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

微控制器的ADC读取传感器R3的值。R3的电阻随着温度升高而减小。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违背安全目标的某些失效模式的探测提供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，声明针对潜伏故障的诊断覆盖率只有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），功能2的表现是当车速高于90 km/h时打开阀1。

如果没有电流经过 l61，阀 1 打开。

相关联的安全目标 2 是“当速度超过 100 km/h 时阀 1 的关闭时间不得长于 y ms”。安全目标被分配为 ASIL C。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。它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 InADC2（表中的安全机制 SM3）监控。轮速由该传感器给出的平均值计算得到。

微控制器没有内部冗余。如果不具备关于复杂元器件的安全故障比例的详细信息，可假定安全故障的保守比例为 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，当探测到多点故障（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 1（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。

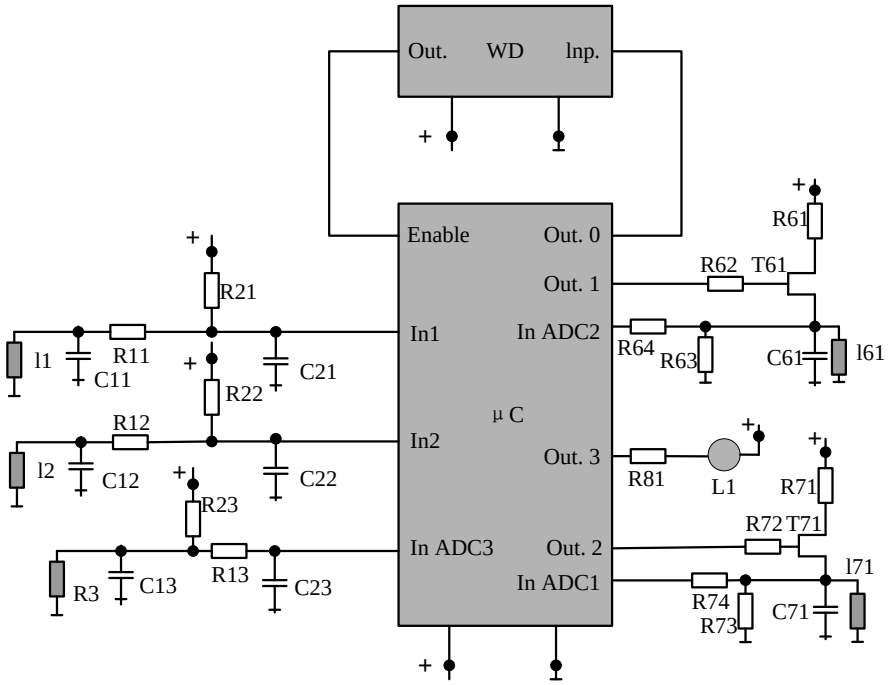
注 2：用于一个给定电子元器件的故障模型可以根据应用而不同。

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 3 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

请注意，下列表格中，安全机制对硬件要素的给定失效模式的覆盖率，称为“失效模式覆盖率”。

组件名															
失效率/FIT		在计算中是否需要考虑的安全相关组件		失效模式	失效率分布		在缺少安全机制时失效模式是否有违背安全目标的潜在可能?	安全机制（多个）允许失效模式违背安全目标吗?	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		在结合其它无关失效时失效模式是否会导致违背安全目标?	探测方法? 安全机制（多个）是否允许预防潜伏的失效模式?	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 节点 1	3		是	开	30%		X	无	0%	0.9					
				关	10%										

					漂 移 0.5	30%									
					漂移 2	30%		X		0%	0.9				
R13 节点 1，节点 2 和节点 7	2		是		开	90%		X	无	0%	1.8				
					关	10%		X		0%	0.2				
R23 节点 1	2		是		开	90%			无						
					关	10%		X		0%	0.2				
C13 的节点 3 和节点 7	2		是		开	20%		X	无	0%	0.4				
					关	80%									
C23	2		否		开	20%									
					关	80%									

WD	20		是		输出卡滞在1	50%						X	无	0%	10
					输出卡滞在0	50%									
T71	5		是		开路	50%		SM1					SM1		
					短路	50%	X		90%	0.25		X		80%	0.45
R71节点2和节点7	2		是		开	90%							无		
					关	10%						X		0%	0.2
R71节点2和节点7	2		是		开	90%							无		
					关	10%						X		0%	0.2
R73	2		否		开	90%									
					关	10%									

R74 节点 2 和节点 7	2		是		开	90%						X	无	0%	1.8
					关	10%						X		0%	0.2
171	5		否		开	70%									
					关	20%									
C71 节点 3	2		是		开	20%						X	无		0.4
					关	80%									
R81	2		否		开	90%									
					关	10%									
L1	10		否		开	90%									
					关	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　　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
总非安全相关	21

安全目标 1 被分配为 ASIL B，对于 ASIL B，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，同时故障度量的计算值为 90%表明潜伏故障度量也被满足。

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：此硬件元器件的目的是提供电气保护。其中一个失效模式是失去电气保护。另一个失效模式在没有安全机制时有违背安全目标的潜在可能。

注 5：计算中不用考虑对违背安全目标没有显著贡献可能性的要素失效。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>2 的多点故障被认为是安全故障。

注 6 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：

$$\lambda_{\mathrm{MPF,L}} = \left[\left(\lambda_{\mathrm{T71}} \times \mathrm{FailureModeDistrib}_{\mathrm{closed\ gate}}\right) - \lambda_{\mathrm{T71RF}}\right] \times \left(1 - \mathrm{FMC}_{\mathrm{LatentFaults}}\right) = [(5 \times 0.1) - 0.05] \times (1 - 0.8) = 0.09$$

注 7：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。

图E. 2 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
失效率分布
在缺少安全机制时失效模式是否有违背安全目标的潜在可能？
安全机制（多个）允许失效模式违背安全目标吗？
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
在结合其它无关失效时失效模式是否会导致违背安全目标？
探测方法？安全机制（多个）是否允许预防潜伏的失效模式？
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 节点 1, 节点 6 及节点 7	2		YES		开	90%		X	SM2	99%	0.018		X	SM2	100 %	0
					关	10%		X		99%	0.002		X		100 %	0
R12 节点 1, 节点 6 及节点 7	2		YES		开	90%		X	SM2	99%	0.018		X	SM2	100 %	0
					关	10%		X		99%	0.002		X		100 %	0

R21 节点 2	2		YES		开	90%		X	SM2	99%	0.018		X	SM2	100%	0
					关	10%		X		99%	0.002		X		100%	0
R22 节点 2	2		YES		开	90%		X	SM2	99%	0.018		X	SM2	100%	0
					关	10%		X		99%	0.002		X		100%	0
C11 节点 1，节点 6 及节点 7	2		YES		开	20%		X	SM2	99%	0.004		X	SM2	100%	0
					关	80%		X		99%	0.016		X		100%	0
C12 接点 1，节点 6 及节点	2		YES		开	20%		X	SM2	99%	0.004		X	SM2	100%	0
					关	80%		X		99%	0.016		X		100	0

7												%		
C21	2	YES	开	20%		SM2				SM2				
			关	80%	X		99%	0.016	X		100%	0		
C22	2	YES	开	20%		SM2				SM2				
			关	80%	X		99%	0.016	X		100%	0		
11	4	YES	开	70%	X	SM2	99%	0.028	X	SM2	100%	0		
			关	20%	X		99%	0.008	X		100%	0		
			漂移 0.5	5%	X		99%	0.002	X		100%	0		
			漂移 2	5%										
12	4	YES	开	70%	X	SM2	99%	0.028	X	SM2	100%	0		
			关	20%	X		99%	0.008	X		100%	0		
			漂移 0.5	5%	X		99%	0.002	X		100%	0		
			漂移 2	5%										

WD	20		YES		输出卡滞在 1	50%						X	none	0%	10
					输出卡滞在 0	50%									
T61	5		YES		开路	50%		SM3					SM3		
					短路	50%	X		90%	0.25		X		100%	0
R61 节点 3 及节点 6	2		YES		开	90%							none		
					关	10%						X		0%	0.2

R62 节点3 及节点 6	2		YES	开	90%							none		
				关	10%						X		0%	0.2
R63	2		NO	开	90%									
				关	10%									
R64 节点 1 及节点 6	2		YES	开	90%						X	none	0%	1.8
				关	10%						X		0%	0.2
161	5		NO	开	70%									
				关	20%									

C61 接点 4 及节点 6	2	YES	开						X	none	0%	0.4%
			关	80%								
R81	2	NO	开	90%								
			关	10%								
L1	10	NO	开	90%								
			关	10%								
μC	100	YES	全部	50%	X	SM4	90%	5	X	SM4	100 %	0
			全部	50%								
							Σ 5.48				Σ 12.80	

总失效率 176 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%

总安全相关 157

总非安全相关 19

安全目标 2 被分配为 ASIL C，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 %表明此度量未被满足，同时故障度量的计算值为 91.6%表明潜伏故障度量得到满足。

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。其它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 ESD 保护。失效模式“开路”意味着失去保护。

注 5：计算中不用考虑对违背安全目标没有显著贡献可能性的要素失效。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>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。

图E. 3 安全目标2

附录F

（资料性附录）

比例因子的应用

比例因子是一种因子，用于组合在随机硬件失效概率度量（PMHF）计算中来自多个来源的失效率。

在 9.4.2.1 中定义的，对每个安全目标的 PMHF 目标值，来自于三个参考来源。

— 表 6，或

— 值得信赖的相似设计原则的现场数据，或

— 应用于值得信赖的相似设计原则中的定量分析技术(使用 8.4.3 给定的失效率)。

为验证硬件设计满足定义的目标值，需基于所涉及的硬件元器件来计算失效率。可基于 8.4.3 所描述的三个来源之一来预估硬件元器件的失效率：

a) 来自公认的行业来源的硬件元器件失效率数据 ，或
b) 基于现场反馈或测试（有足够的置信度水平）的统计，或
c) 建立在基于定量和定性论据的工程方法上的专家判断

因此，在计算中，不同的失效率来源可以被用于相关项的不同硬件元器件。

让 Ta、Tb 和 Tc 作为 PMHF 目标值定义的三个可能来源，Fa、Fb 和 Fc 作为硬件元器件失效率预估的三个可能来源。让$\pi_{Fi\to Fj}$作为介于 Fi 和 Fj 之间的比例因子。该因子可用于换算基于 Fi 的硬件元器件失效率和基于 Fj 的失效率的比例关系，如方程（F.1）所示：

$$\pi_{Fi\to Fj} = \frac{\lambda_{k.Fj}}{\lambda_{k.Fi}} \tag{F.1}$$

这里

$\lambda_{k.Fj}$ 是使用 Fj 作为失效率来源的硬件元器件的失效率；

$\lambda_{k.Fi}$ 是使用 Fi 作为失效率来源的某些硬件元器件的失效率。

在此情况下，已知的比例因子使基于 Fi 的类似硬件元器件失效率能换算成基于 Fj 的失效率，如方程（F.2）所示：

$$\lambda_{l,Fj} = \pi_{Fi\to Fj} \times \lambda_{l,Fi} \tag{F.2}$$

表 F1 表示目标值与失效率之间的可能组合。

注 1：表 6 的目标值基于使用手册数据并且在假设手册数据是非常悲观的前提下计算的。

注 2：如果目标值和硬件元器件失效率的数据源是相似的，那么不需要比例换算。

表 F1 目标值和失效率的来源的可能组合产生用于计算的一致失效率

硬件元器件失效率数据来源	目标值的数据源		
	表 6 9.4.2.1 a)	现场数据 9.4.2.1 b)	定量分析 9.4.2.1 c)
标准数据库 8.4.3 a)	$\lambda_{k.Fa}$ [a]	$\lambda_{k,Fb} = \pi_{Fa \to Fb} \times \lambda_{k,Fa}$	b
统计 8.4.3 b)	$\lambda_{k,Fa} = \pi_{Fb \to Fa} \times \lambda_{k,Fb}$	$\lambda_{k.Fb}$	b
专家判断 8.4.3 c)	$\lambda_{k,Fa} = \pi_{Fc \to Fa} \times \lambda_{k,Fc}$	$\lambda_{k,Fb} = \pi_{Fc \to Fb} \times \lambda_{k,Fc}$	b
[a] 对某些类型的硬件元器件，不同的手册对这些相同类型的硬件元器件给出不同的失效率预估。因此，比例因子可用不同手册来比例换算硬件元器件的失效率。 [b] 为了保持方法的一致性，此失效率和用于计算目标值的失效率有相同的来源。			

如果有足够的证据证明在目标值的两个可能来源之间存在一个因子，那么比例换算是可行的。

例如，如果对“上一代”系统存在足够的数据，它的失效率可认为代表了所考虑的相关项。

示例 1：可提供证据证明 99%置信度的$\frac{10^{-8}}{\mathrm{h}}$和 70%置信度的$\frac{10^{-9}}{\mathrm{h}}$是相似的。因此，可用比例因子$\pi_{Fa \to Fb} = \left(\frac{10^{-9}}{\mathrm{h}}\right) \div \left(\frac{10^{-8}}{\mathrm{h}}\right) = \frac{1}{10}$或其它方法，将认为具有 99%置信度的基于公认的工业资料来源的失效率比例换算为具有 70%置信度的基于统计学的失效率。

注 3：根据经验，参照 8.4.3，基于公认的工业数据来源的失效率可以被考虑为 99%的置信度。

示例 2：根据上一个设计，已获得根据数据手册和质保数据计算得到的失效率，我们知道：

$$\frac{\lambda_{\mathrm{handbook}}}{\lambda_{\mathrm{warranty}}} = \pi_{Fb \to Fa} = 10 \qquad \text{(F.3)}$$

这里：

$\lambda_{\mathrm{handbook}}$ 是根据数据手册计算得到的失效率

$\lambda_{\mathrm{warranty}}$ 是根据质保数据计算得到的失效率

$\pi_{Fb \to Fa}$是比例换算的结果

如果在一个新设计中，除了我们只有质保数据的硬件元器件（硬件元器件 1）外，我们使用手册数据来确定失效率，那么我们可以根据下面的比例方法确定该硬件元器件的手册数

据：

$$\lambda_{1,\text{handbook}} = \pi_{Fb \to Fa} \times \lambda_{1,\text{warranty}} \quad \text{(F.4)}$$

这里：

$\lambda_{1,\text{handbook}}$ 是使用手册数据的硬件元器件 1 的失效率

$\lambda_{1,\text{warranty}}$ 是使用质保数据的硬件元器件 1 的失效率

例如，如果$\lambda_{1,\text{warranty}} = \frac{9\times10^{-9}}{\text{h}}$，那么$\lambda_{1,\text{handbook}}$ 可以按$(9 \times 10^{-9}) \times 10 = \frac{9\times10^{-8}}{\text{h}}$来计算。

使用该$\lambda_{1,\text{handbook}}$ ， 可做到对由随机硬件失效导致违背安全目标的一致评估。