ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.6—2006/IEC 61508-6:2000

电气/电子/可编程电子安全相关系统的功能安全　第6部分:GB/T 20438.2和GB/T 20438.3的应用指南

Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 6:Guidelines on the application of GB/T 20438.2 and GB/T 20438.3

(IEC 61508-6:2000,IDT)

2006-07-25 发布　　2007-01-01 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

目　次

前　言

GB/T 20438 由下列 7 部分构成：

——第 1 部分：一般要求；

——第 2 部分：电气/电子/可编程电子安全相关系统的要求；

——第 3 部分：软件要求；

——第 4 部分：定义和缩略语；

——第 5 部分：确定安全完整性等级的方法示例；

——第 6 部分：GB/T 20438.2 和 GB/T 20438.3 的应用指南；

——第 7 部分：技术和措施概述。

本部分是 GB/T 20438 的第 6 部分。

本部分等同采用国际标准 IEC 61508-6:2000《电气/电子/可编程电子安全相关系统的功能安全 第 6 部分：IEC 61508-2 和 IEC 61508-3 的应用指南》(英文版)。

附录 A、附录 B、附录 C、附录 D、附录 E 为资料性附录。

本部分与 IEC 61508-6:2000 在技术内容上没有差异，为便于使用做了下列编辑性修改：

a) 将“IEC 61508”改为“GB/T 20438”。

b) “本国际标准”一词改为“本标准”。

c) 删除国际标准中 1.3 的注，因为此注所表述的是 IEC 61508 在美国和加拿大等国的应用情况，与我国的实际不符，所以删除。

d) 用小数点“.”代替原标准中作为小数点的逗号“,”。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量和控制标准化技术委员会(SAC/TC 124)归口。

本部分由机械工业仪器仪表综合技术经济研究所负责起草。

本部分主要起草人：郑旭、冯晓升、梅恪、王莉、欧阳劲松等。

引　言

由电气和电子器件构成的系统，多年来在许多领域中执行其安全功能，以计算机为基础的系统（一般指可编程电子系统（PES））在许多领域中用于非安全目的，但也越来越多地用于安全目的，为使计算机系统技术更有效安全的使用，有必要进行安全方面的指导。

GB/T 20438 针对由电气或电子和可编程电子部件构成的、起安全作用的电气/电子/可编程电子系统（E/E/PES）的整体安全生命周期，提出了一个通用的方法。建立统一的方法的目的是为了针对以电子为基础的安全相关系统提出一种一致的、合理的技术方针，主要目标是促进应用领域标准的制定。

在许多情况下，可用多种基于不同技术的防护系统来保证安全（如机械的、液压的、气动的、电气的、电子的、可编程电子的，等等）。从安全战略角度，不仅要考虑各独立系统中所有元器件的问题（如传感器、控制器、执行器等），而且要考虑由所有安全相关系统构成的组合安全相关系统的问题。因此 GB/T 20438对电气/电子/可编程电子（E/E/PE）安全相关系统进行了规定。GB/T 20438 还提出了一个框架，在这个框架内，基于其他技术的安全相关系统也可同时被考虑进去。

在各种应用领域里，存在着许多潜在的危险和风险，包含的复杂性也各不相同，从而需应用不同的 E/E/PES。对每个特定的应用，则根据应用的不同而确定所需的安全量。GB/T 20438 仅是使这些量值规范化。

GB/T 20438

——考虑了当使用 E/E/PES 执行安全功能时，所涉及到的整体安全生命周期、E/E/PES 安全生命周期以及软件安全生命周期的各阶段（如初始构思，整个设计、实现、运行、维护及停用）。

——针对飞速发展的技术，建立一个足够健壮而广泛的能满足今后发展需要的框架。

——有利于促进 E/E/PE 安全相关系统在不同领域中相关标准的制订，各应用领域和交叉应用领域相关标准应在 GB/T 20438 的框架下制定，使之具有高水平的一致性（如基础原理，术语等的一致性）并将既安全又经济。

——为达到 E/E/PE 安全相关系统所需的功能安全，提供了编制安全要求规范的方法。

——使用了一个安全完整性等级，此安全完整性等级规定了 E/E/PE 安全相关系统要实现的安全功能的目标安全完整性等级。

——采用了一种基于风险的方案来确定安全完整性等级要求。

——建立了 E/E/PE 安全相关系统的数值目标失效量，这些量都同安全完整性等级相联系。

——建立了危险失效模式中目标失效量的一个下限，此下限是对单一 E/E/PE 安全相关系统的要求。

这些系统运行在：

1）　低要求操作模式下，为了执行它的设计功能，一旦要求时，就把下限设定成平均失效概率为 10^{-5}；

2）　高要求操作模式或者连续操作模式下，下限设定成危险失效概率为 10^{-9}/h。

注：单一 E/E/PE 安全相关系统不一定是单通道结构。

——采用广泛的原理，技术和措施以达到 E/E/PE 安全相关系统的功能安全，但不使用失效-安全的概念，这个概念是在很好定义了失效模式，并且复杂性相对较低时的一个数值。由于 E/E/PE安全相关系统的复杂性均在 GB/T 20438 范围之内，因此不适用失效-安全的概念。

电气/电子/可编程电子安全相关系统的功能安全　第6部分:GB/T 20438.2和GB/T 20438.3的应用指南

1　范围

1.1　本部分包括GB/T 20438.2与GB/T 20438.3的信息以及指南:

——附录A中阐述了GB/T 20438.2及GB/T 20438.3的要求简述,以及应用过程中的功能步骤。

——附录B列举了如何计算硬件失效概率。阅读时要结合GB/T 20438.2—2006的7.4.3和附录C以及本部分的附录D。

——附录C给出了诊断覆盖率的计算示例,阅读时要结合GB/T 20438.2—2006的附录C。

——附录D阐述了将硬件共同原因失效率量化的方法论。

——附录E给出了GB/T 20438.3—2006附录A中规定的在安全完整性等级2和3时软件安全完整性表的应用示例。

1.2　GB/T 20438.1、GB/T 20438.2、GB/T 20438.3和GB/T 20438.4是基础安全标准,虽然它们不适用于简单的E/E/PE安全相关系统(见GB/T 20438.4—2006中的3.4.4),作为基础的安全标准,根据IEC导则104和ISO/IEC导则51中包含的原则,相关的技术委员会在制定标准时应使用它们。GB/T 20438也可独立使用。

1.3　若适用,技术委员会在制定其标准时都应使用基础安全标准。也就是说,本基础安全标准涉及的要求、测试方法或测试条件,只有在相关技术委员会制定标准时加以引用或包含时,才能得到应用。

1.4　图1显示了GB/T 20438的总体框架并指出了本部分在实现E/E/PE安全相关系统功能安全时的作用。

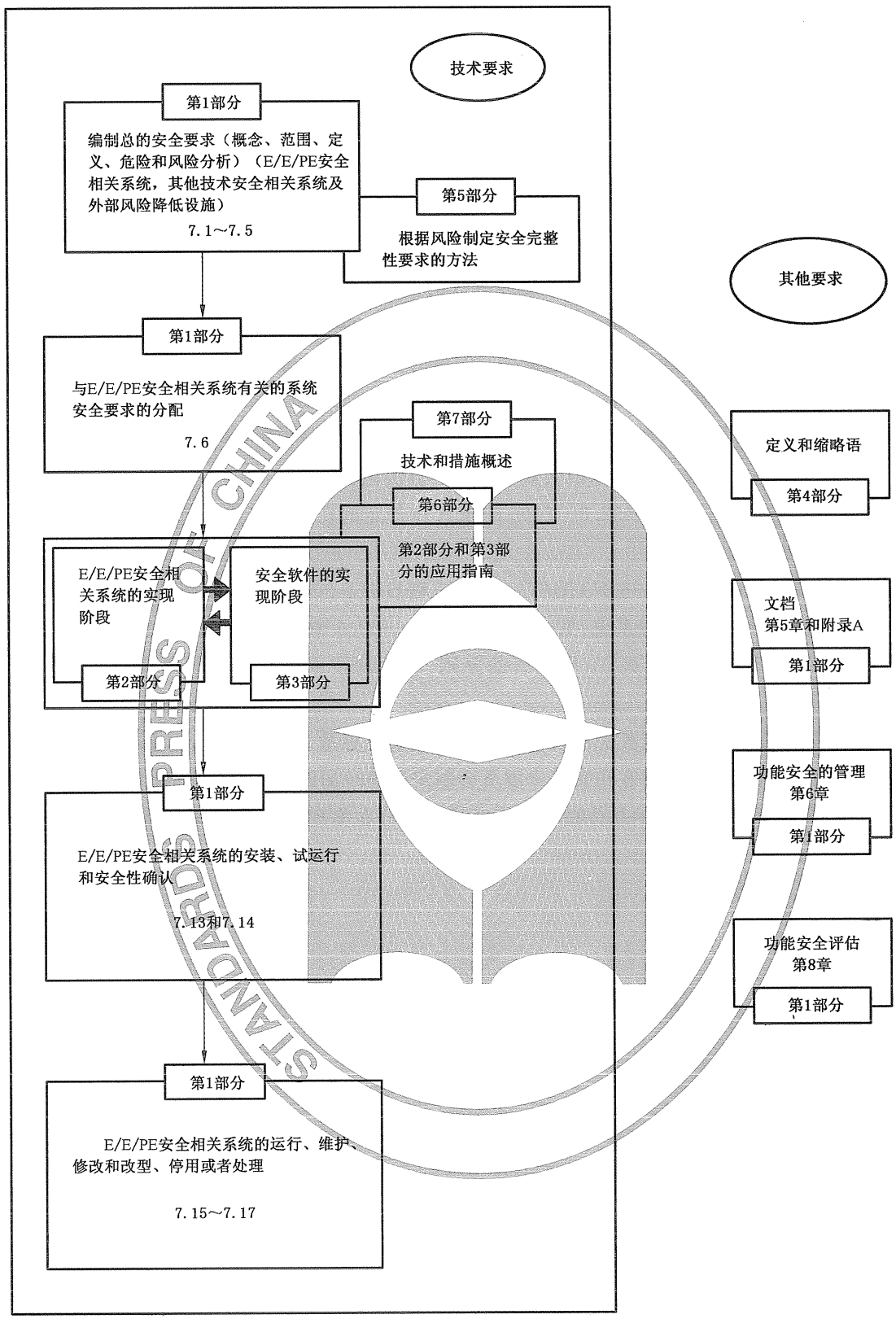


图 1　GB/T 20438 的总体框架

2 规范性引用文件

下列文件中的条款通过 GB/T 20438 的本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB/T 20438(所有部分) 电气/电子/可编程电子安全相关系统的功能安全(GB/T 20438—2006，IEC 61508，IDT)

IEC 导则 104:1997 安全出版物的编写及基本安全出版物和分类出版物的应用

IEC/ISO 导则 51:1990 安全方面 在标准中引入安全条款的指南

3 定义和缩略语

见 GB/T 20438.4。

附 录 A
（资料性附录）
GB/T 20438.2 和 GB/T 20438.3 的应用

A.1 概述

机械、过程成套设备以及其他设备在工作不正常的情况下（例如电气、电子或可编程电子设备的失效）有可能产生诸如火灾、爆炸、辐射超剂量、机械困油等危险事件，因此对工人和环境而言存在一定风险。失效既可能因设备的物理故障（如引起随机硬件失效），也可能因为系统故障（例如，在系统的设计和规范中的人为错误在一些特别输入组合的情况下，会导致系统失效）或者因为某个环境条件而产生。

GB/T 20438.1 提供了一个基于风险方法的总体框架，以便防止和/或控制电气、电子或者可编程电子设备中的失效。

GB/T 20438 的总目标就是确保设备、仪器安全地自动运行，其中关键目标就是防止：

——引发其他事件的控制系统失效，这些失效将导致（火灾、有毒物质泄露、机械设备多次冲击等）危险；并且

——保护系统（如紧急制动系统）中未检测到的失效使系统不能在需要时正常执行一次安全动作。

GB/T 20438.1 要求在过程或机器级执行一次危险和风险分析，从而确定在应用中满足风险准则所必需的风险降低量。风险是基于危险事件的后果（或严重性）和频率（或概率）的评估。

GB/T 20438.1 还需要由风险分析建立的风险降低量来确定需要一个或几个安全相关系统[1)]，以及它们需要什么样的安全功能（每个都有一个规定的安全完整性[2)]）。

GB/T 20438.2 和 GB/T 20438.3 涉及了 GB/T 20438.1 分配给任意一个被指定为 E/E/PE 安全相关系统的安全功能和安全完整性要求，并建立安全生命周期活动的要求，这些要求：

——将在硬件及软件的规范、设计、修改中使用；并且

——重点是防止和/或控制硬件以及系统的失效的方法（E/E/PE 和软件安全生命周期[3)]）。

GB/T 20438.2 和 GB/T 20438.3 并没有给出安全完整性哪个水平适合给定要求的允许风险的指南，这取决于多种因素，包括应用的类别、其他系统执行安全功能的程度及社会、经济因素等（见 GB/T 20438.1及 GB/T 20438.5）。

GB/T 20438.2 与 GB/T 20438.3 的要求包括：

——措施与技术的应用[4)]，在使用预防方法避免系统失效[5)]时，可按安全完整性等级对它们进行分类；并且

——利用故障检测、冗余和结构特征（如多样性）这些设计特征控制系统失效（包括软件失效）和随机硬件失效。

---

1) 功能安全所需要的并包括一个或多个电气（机电）、电子、可编程电子（E/E/PE）设备的系统被指定为 E/E/PE 安全相关系统，并包括所有运行安全功能所必需的设备（见 GB/T 20438.4—2006 的 3.4.1）。

2) 安全完整性规定为四个独立的水平之一。安全完整性等级 4 为最高级，安全完整性等级 1 为最低级（见 GB/T 20438.1—2006 的 7.6.2.9）。

3) 为了清晰地构建 GB/T 20438 的要求，决定使用一种开发过程模型，按照已定义好的、很少出现重复的顺序对要求进行排序（有时称为瀑布模型）。但是，值得强调的是，倘若在工程项目中安全计划能给出一种等价的陈述，就可以使用任何生命周期方案（见 GB/T 20438.1—2006 的第 6 章）。

4) 在 GB/T 20438.2—2006 和 GB/T 20438.3—2006 的附录 A 和附录 B 的表中给出了每一安全完整性等级所需的技术和措施。

5) 系统失效一般不能被量化，原因包括：在硬件和软件中存在规范和设计故障；考虑环境（如温度）引起的失效以及操作故障（如不良界面）。

GB/T 20438.2 中，满足危险随机失效的安全完整性目标的保证是基于：

——硬件故障裕度要求(见 GB/T 20438.2—2006 的表 2、表 3)；并且

——使用适当的数据，经过可靠性分析来确定子系统与部件的诊断覆盖率和检验测试的频率。

在 GB/T 20438.2 与 GB/T 20438.3 中满足系统失效要求的安全完整性目标的保证可由以下获得：

——正确应用安全管理规程；

——任用合格的人员；

——应用规定的安全生命周期活动，包括规定的技术和措施[6]；

——一个独立的功能安全评估[7]。

总目标是要确保与安全完整性相应的残余系统故障，不会导致 E/E/PE 安全相关系统的失效。GB/T 20438.2 为 E/E/PE 安全相关系统的硬件[8](包括传感器、最终元件)达到安全完整性提供要求。需要防止随机硬件失效和系统硬件失效的技术和措施。如上所述，它们包括适当的措施以避免故障和控制失效。在那种功能安全需要人员动作的场合，给出了对操作员界面的要求。在 GB/T 20438.2 中还规定了用于检测随机硬件失效基于软件和硬件的诊断测试技术和措施(例如多样性)。

GB/T 20438.3 为软件——嵌入式软件(包括诊断故障检测服务)和应用软件达到安全完整性提供要求。由于还不知道有什么方法来证明适度复杂的安全软件中不存在故障，特别是不存在规范和设计故障，所以 GB/T 20438.3 需要故障避免(质量保证)和故障裕度方案的组合(软件结构)。GB/T 20438.3需要采用如下软件工程原理：自顶向下的设计、模块化、验证开发生命周期的每一个阶段、经验证的软件模块和软件模块库、清空文档以便验证和确认。不同软件层需要不同的保证，以确保这些以及相关原理已经被正确的应用。

软件的开发者可与或不与开发整个 E/E/PES 的组织分离开。无论哪种情况下，密切协作都是必要的，特别是在可编程电子的结构开发中，需要从安全效果出发考虑硬件和软件结构之间的折衷方案(见 GB/T 20438.2—2006 图 4)。

A.2 GB/T 20438.2 应用中的功能步骤

GB/T 20438.2 应用中的功能步骤如图 A.1 和图 A.2 所示，GB/T 20438.3 应用中的功能步骤如图 A.3 所示。

GB/T 20438.2 应用中的功能步骤(见图 A.1 和图 A.2)如下所示：

a) 获得安全要求的分配(见 GB/T 20438.1)，在开发 E/E/PES 的过程中更新相应的安全计划编制。

b) 对于每个安全功能，确定 E/E/PES 的安全要求，包括安全完整性要求(见 GB/T 20438.2—2006 的 7.2)。给软件分配要求并提交供应商和/或开发者以便应用 GB/T 20438.3。

注：在这一阶段需要考虑 EUC 控制系统和 E/E/PE 安全相关系统中同时发生的失效的概率(见 GB/T 20438.1—2006 的 7.5.2.4)。它们可能是由于受诸如相似环境影响的共同原因失效的部件所引起的结果。这种失效的存在会导致比预计中更高的残余风险，除非已对其作了适当的陈述。

c) 启动 E/E/PE 安全确认计划编制阶段(见 GB/T 20438.2—2006 的 7.3)。

d) 规定 E/E/PE 逻辑子系统、传感器和最终元件的结构(配置)，与软件供应商/开发者一起复审，硬件和软件结构以及硬件和软件之间折衷方案的安全含义(见 GB/T 20438.2—2006 的图

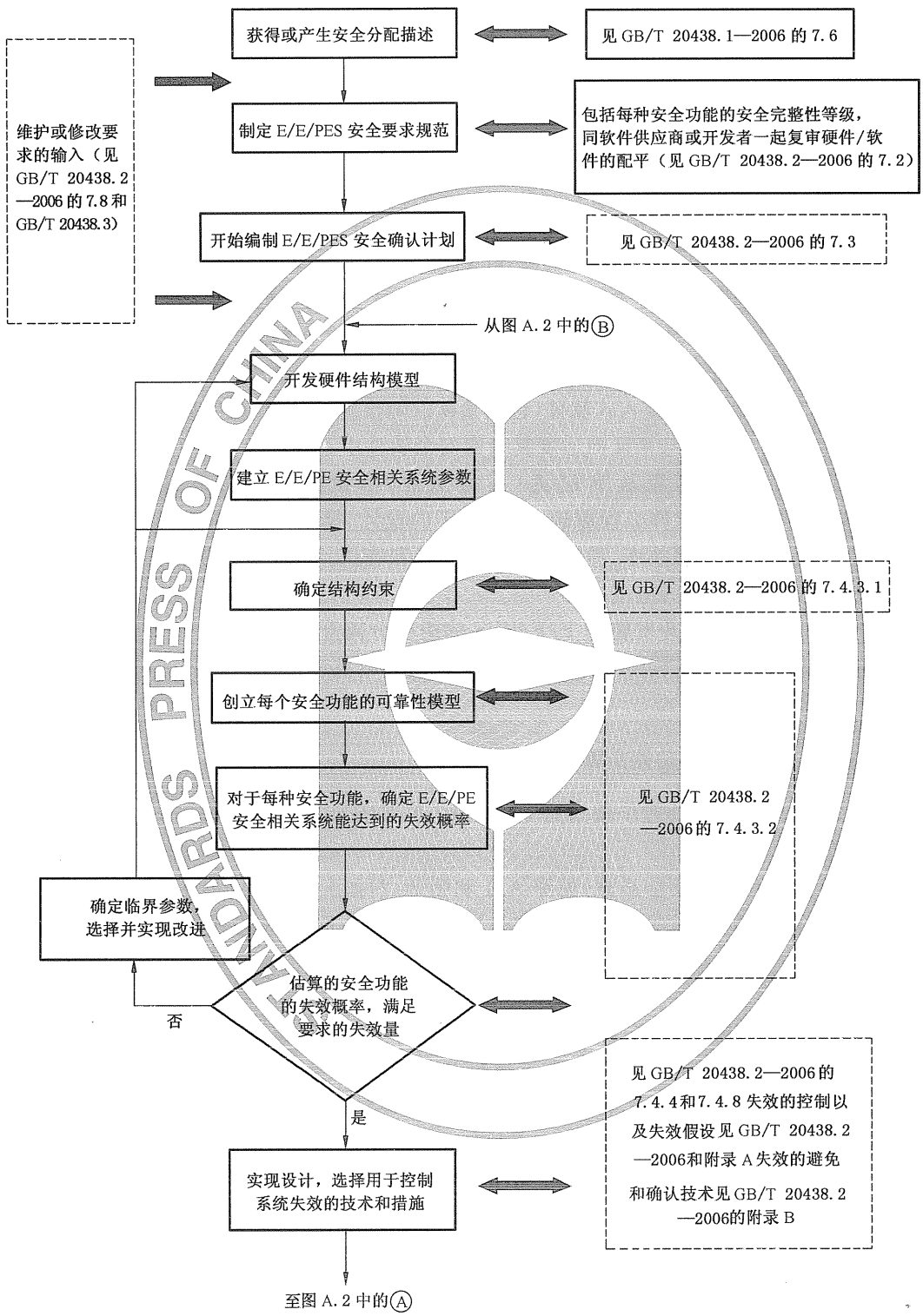
6) 如果在编制安全计划过程中合理性证明已文档化，GB/T 20438 中规定的那些措施可以被替代(见 GB/T 20438.1—2006 的第 6 章)。

7) 独立评估不一定是第三方评估(见 GB/T 20438.1—2006 的第 8 章)。

8) 包括固定的内置软件或软件等效物(也称为固件)，如专用集成电路。

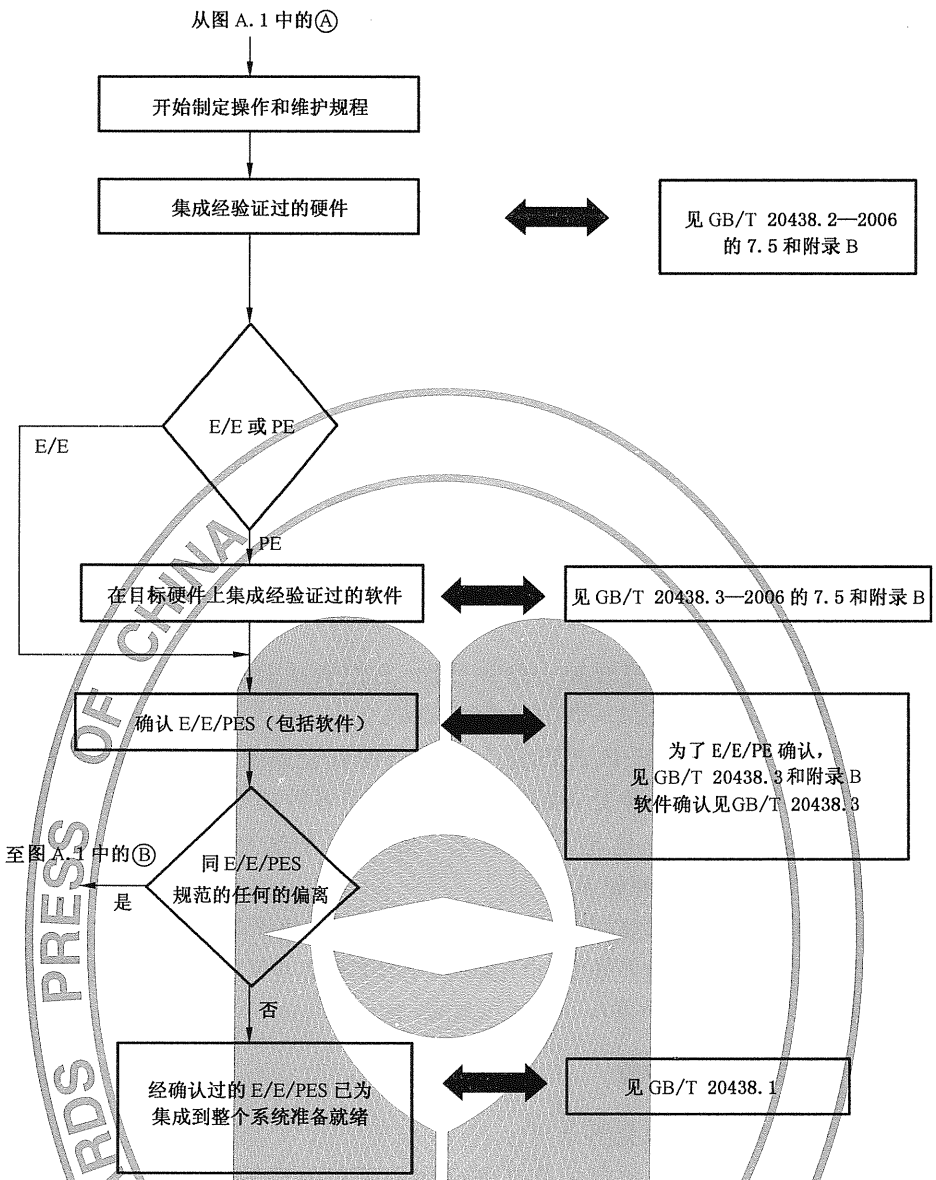
4)。如果需要将重复此步骤。

e) 开发 E/E/PE 安全相关系统硬件结构模型，通过分别测试每个安全功能开发硬件的结构模型并确定用来执行这些功能的子系统(部件)。



注：对于 PE 系统，针对软件的活动将并行发生(见图 A.3)。

图 A.1 GB/T 20438.2 的应用



注：对 PE 系统而言，软件的活动是并行的（见图 A.3）。

图 A.2　GB/T 20438.2 的应用

f) 建立 E/E/PE 安全相关系统中使用的每个子系统（部件）的系统参数。确定每个子系统（部件）的：

——失效的检验测试时间间隔，这些失效是不会自动被显现出来的；

——平均恢复时间；

——诊断覆盖率（见 GB/T 20438.2—2006 的附录 C）；

——失效概率；

——安全失效分数（见 GB/T 20438.2—2006 的附录 C）。

g) 确定结构约束（见 GB/T 20438.2—2006 的表 2、表 3）。

h) 创建 E/E/PE 安全相关系统需要执行的每个安全功能的可靠性模型。

注：可靠性模型是一个数学公式，用以表示与设备和使用条件有关的可靠性和相关参数之间的关系。

i) 使用适当的技术计算每个功能安全的可靠性期望值，将上面 b）项中确定的目标失效量结果同 GB/T 20438.2—2006 中表 2、表 3 的要求进行比较（见 GB/T 20438.2—2006 的 7.4.3.1）。如

果期望的可靠性与目标失效量不同和/或不符合 GB/T 20438.2—2006 中表 2、表 3 的要求，则：

——在可能时改变一个或多个子系统参数(返回到上面的 f))；和/或

——改变硬件结构(返回到上面的 d))。

注：有多种建模方法，分析人员应该选择最适合的方法(见 GB/T 20438.2—2006 的 7.4.3.2.2 注 9 中所列的可使用的几种方法)。

j) 实现 E/E/PE 安全相关系统的设计。选择用来控制系统硬件失效、受环境影响产生的失效和操作失效的技术和措施(见 GB/T 20438.2—2006 的附录 A)。

k) 在目标硬件上集成(见 GB/T 20438.2—2006 的 7.6 及附录 B)经验证过的软件(见 GB/T 20438.3)时为用户和维护人员制定系统操作规程(见 GB/T 20438.2—2006 的 7.6 及附录 B)。包括软件方面(见上面的 f))。

l) 与软件开发者(见 GB/T 20438.3—2006 的 7.7)一起确认 E/E/PES(见 GB/T 20438.2—2006 的 7.7 和附录 B)。

m) 把硬件和 E/E/PES 安全确认的结果移交给系统工程师，以便进一步集成到整个系统中。

n) 如果在使用寿命期限内需要维护或修改 E/E/PES，则将适当地重新启动 GB/T 20438.2(见 GB/T 20438.2—2006 的 7.8)。

在整个 E/E/PES 安全生命周期将开展一系列活动，它们包括验证(见 GB/T 20438.2—2006 的 7.9)和功能安全评估(见 GB/T 20438.1—2006 的第 8 章)。

在应用上述步骤的时候，应选择 E/E/PES 适合于要求的安全完整性等级的技术和措施。为了帮助选择，已经编制好了一些表，针对 4 种安全完整性等级列出了各种技术和措施(GB/T 20438.2—2006 的 7.6 和附录 B)。在进一步参考这些信息源时，交叉参考这些表可总览每种技术和措施(见 GB/T 20438.7—2006 的附录 A 和附录 B)。

附录 B 提供了一种可行的计算 E/E/PE 安全相关系统硬件失效概率的技术。

注：在应用上述步骤时如果在编制安全计划过程中合理性证明已文档化，GB/T 20438 中规定的那些措施可以被替代(见 GB/T 20438.1—2006 的第 6 章)。

A.3 GB/T 20438.3 应用中的功能步骤

GB/T 20438.3 的功能步骤如下(见图 A.3)：

a) 获得 E/E/PE 安全相关系统的要求及其安全计划编制的相关部分(见 GB/T 20438.3—2006 的 7.3)。在开发软件期间更新安全计划使之更加恰当。

注 1：早期生命周期阶段已经：

——规定了要求的安全功能，以及相关的安全完整性等级(见 GB/T 20438.1—2006 的 7.4 和 7.5)；

——为指定的 E/E/PE 安全相关系统分配了安全功能(见 GB/T 20438.1—2006 的 7.8)；

——给每个 E/E/PE 系统中的软件分配功能(见 GB/T 20438.2—2006 的 7.2)。

b) 为所有分配给软件的安全功能确定软件结构(见 GB/T 20438.3—2006 的 7.4 及附录 A)。

c) 与 E/E/PES 供应商/开发者一起复审软件和硬件结构，及软件和硬件之间进行折衷方案的安全含义(见 GB/T 20438.2—2006 的图 4)。当需要时应进行重复。

d) 开始编制软件安全验证和确认计划。

e) 根据以下条件设计、开发、验证或测试软件：

——软件安全计划编制；

——软件安全完整性等级；和

——软件安全生命周期。

f) 完成最终的软件验证活动，并在目标硬件上集成经验证过的软件(见 GB/T 20438.3—2006 的

7.5),并行开发用户和维护人员在操作系统时所依据的规程的软件方面(见 A.2 的 k)和 GB/T 20438.3—2006 的 7.6)。

g) 与硬件开发者一道(见 GB/T 20438.2—2006 的 7.7)确认已集成的 E/E/PE 安全相关系统中的软件(见 GB/T 20438.3—2006 的 7.7)。

h) 将软件安全确认的结果移交给系统工程师,以便进一步集成到整个系统中。

i) 如果在使用寿命期限内需要对 E/E/PES 软件进行修改,则应重新启动 GB/T 20438.3 的这个相应阶段。

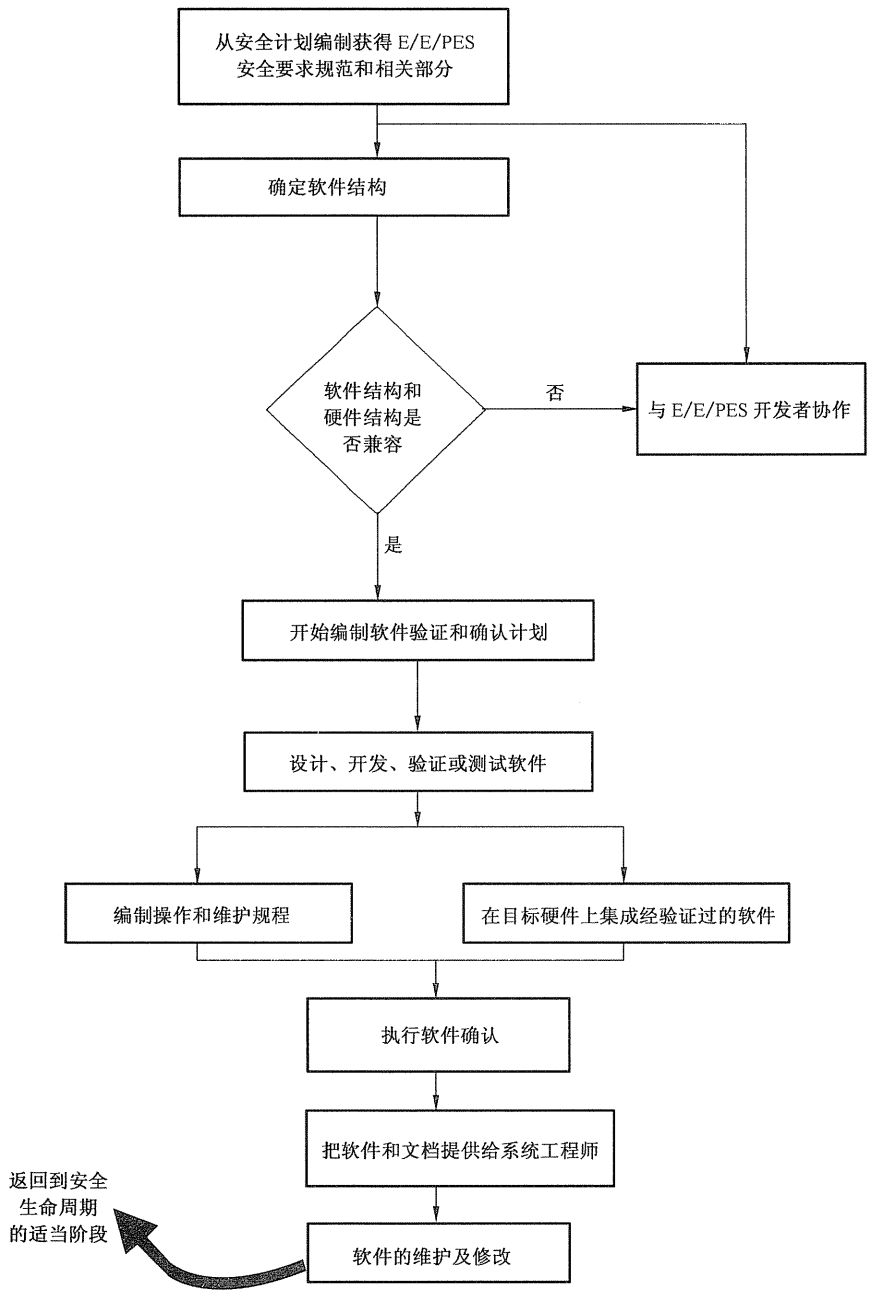


图 A.3 GB/T 20438.3 的应用

在整个软件安全生命周期将开展一系列活动,它们包括验证(见 GB/T 20438.3—2006 的 7.9)和功能安全评估(见 GB/T 20438.3—2006 的第 8 章)。

在应用上述步骤时,应选择适合于要求的安全完整性等级的软件安全技术和措施。为了帮助选择,

已编制了一些表，针对4种安全完整性等级列出了各种技术和措施（见GB/T 20438.3—2006的附录A）在进一步参考这些信息源时，交叉参考这些表可总览每种技术和措施（见GB/T 20438.7—2006的附录C）。

安全完整性表的应用实例在附录E中给出。并且GB/T 20438.7中包括了确定预开发软件的软件安全完整性的概率法（见GB/T 20438.7—2006的附录D）。

注：在应用上述步骤时，如果在编制安全计划过程中合理性证明已文档化，GB/T 20438中规定的那些措施可以被替代（见GB/T 20438.1—2006的第6章）。

附 录 B
（资料性附录）
硬件失效概率评估技术示例

B.1 概述

本附录提供了计算用来根据 GB/T 20438.1、GB/T 20438.2 和 GB/T 20438.3 安装的 E/E/PE 安全相关系统的硬件失效概率的技术。本附录提供的信息是参考性资料，不应解释为可以使用的唯一的评价技术。但是，本方法为评估 E/E/PE 安全相关系统的能力提供了一种相对简单的方法。

注 1：例如，在 ANSI/ISA S 84.01:1996《过程工业领域安全仪表系统的应用》中描述了其他技术。

有很多技术可用来分析 E/E/PE 安全相关系统硬件安全完整性，其中比较常用的两种技术是可靠性框图（见 GB/T 20438.7—2006 中 C.6.5）和马尔可夫模型（见 GB/T 20438.7—2006 中 C.6.4）。如果正确使用，这两种方法会得到相似的结果，但对于复杂的可编程电子子系统的情况（如使用多通道交叉表决和自动测试的情况）与马尔可夫模型相比，使用可靠性框图时的精确性有所下降。

这种精度的损失对于整个 E/E/PE 安全相关系统来说以及考虑在分析中使用可靠性数据的精度时不太重要。例如，在分析 E/E/PE 安全相关系统的硬件安全完整性时，现场设备经常起主要作用。仅在特殊情况下确定精度损失才是重要的。当测量复杂可编程电子子系统时，可靠性框图得到的硬件安全完整性值比马尔可夫模型得到的测量结果更差（即可靠性框图得到的硬件失效概率值比较大），本附录使用了可靠性框图。

在 EUC 控制系统失效对 E/E/PE 安全相关系统提出一次要求，危险事件的发生概率仍然取决于 EUC 控制系统的失效概率的情况下，有必要考虑 EUC 控制系统和 E/E/PE 安全相关系统部件因共同原因失效机制产生的同时失效的可能性。存在这样的故障就会导致比预期更大的残余风险，除非已作适当的论述。

计算基于以下假设：

——在要求时子系统出现失效的平均概率低于 10^{-1}，或者子系统每小时的失效概率小于 10^{-5}。

——在系统寿命内部件失效概率为常量。

——传感器（输入）子系统包含实际的传感器、其他部件、接线，但不包括通过表决或其他处理首先组合信号的那些部件（例如，对于双传感器通道，其配置如图 B.1 所示）。

——逻辑子系统包括首先组合信号的部件和把最终信号传递给最终元件子系统的所有其他部件。

——最终元件子系统包括用来处理来自逻辑子系统的最终信号的所有部件和连线，还包括最终执行元件。

——对于子系统中的单个通道，硬件失效率被当作计算和表格的输入（例如，如果使用 2oo3 传感器，失效率则是指单个传感器的失效率，并且单独计算 2oo3 的影响）。

——在一个经表决过的组中所有通道具有相同的失效率和诊断覆盖率。

——子系统中一个通道的硬件总失效率为此通道危险失效率和安全失效率的总和（假设两者是相同的）。

注 2：本假设将影响安全失效分数（见 GB/T 20438.2—2006 中的附录 C），但安全失效分数不影响本附录中给出的失效概率的计算值。

——每个安全功能都已经过很好的检验测试和修复(即:所有未检测到的失效可由检验测试检测到),非完全检验测试的效应,可以查询 B.2.5。

——检验测试的间隔至少要比诊断测试的间隔大一个数量级。

——对于每个子系统都有一个检验测试间隔以及平均恢复时间。

注 3:平均恢复时间已经在 GB/T 20438.2—2006 的 7.4.3.2.2 的注 5 中定义了,它包含了检测失效所需的时间。本附录中,假设检测到和未检测到的失效的平均恢复时间包括诊断测试间隔,但不包括检验测试间隔。对于未检测到的失效,计算中使用的平均恢复时间不包括诊断测试间隔,但是因为平均恢复时间总是要加到检验测试间隔中(比诊断测试的间隔至少要大一个数量级),因此误差并不重要。

——对于已知的失效可采取多个修理班组同时进行处理。

——预计的要求间隔至少比平均恢复时间大一个数量级。

——对于所有在低要求操作模式下运行的子系统以及在高要求或连续操作模式下工作的 1oo2、1oo2D、2oo3 表决组,诊断覆盖率规定的失效分数,在平均恢复时间内已被检测和修复,并用来决定硬件安全完整性的需求。

例如:假设平均恢复时间为 8 h,它一般包括小于 1 h 的诊断测试间隔,其余为实际修理时间。

注 4:对 1oo2、1oo2D、2oo3 表决组,假设任何修理均在线进行。配置一个 E/E/PE 安全相关系统就可在检测到任何故障时使 EUC 进入一种安全状态,从而可以减小要求的平均失效概率,提高程度取决于诊断覆盖率。

——对于在高要求或连续操作模式下工作的 1oo2、1oo2D、2oo3 表决组,E/E/PE 安全相关系统在检测到危险故障后,总可达到安全状态。为了达到这种状态,要求之间的预计间隔至少要比诊断测试间隔大一个数量级,或者诊断测试间隔与达到安全状态所需时间的总和少于过程安全时间。

注 5:过程安全时间已在 GB/T 20438.2—2006 的 7.4.3.2.5 中定义为 EUC 或 EUC 控制系统发生失效(具有引起一次危险事件的潜在可能)至未能执行安全功能就会发生危险事件之间的时段。

——当电源失效,不能对断电跳闸 E/E/PE 安全相关系统提供电力时,系统脱扣到安全状态,此时电源不会对 E/E/PE 安全相关系统要求的平均失效概率产生影响;如果系统需通电跳闸,或者电源的失效模式能引起 E/E/PE 安全相关系统不安全工作,电源应包括在评价内容之中。

——当使用术语通道时,它只限于所讨论的系统的那部分,通常指传感器子系统、逻辑子系统或最终元件子系统。

——缩略的术语及符号在表 B.1 中有所描述。

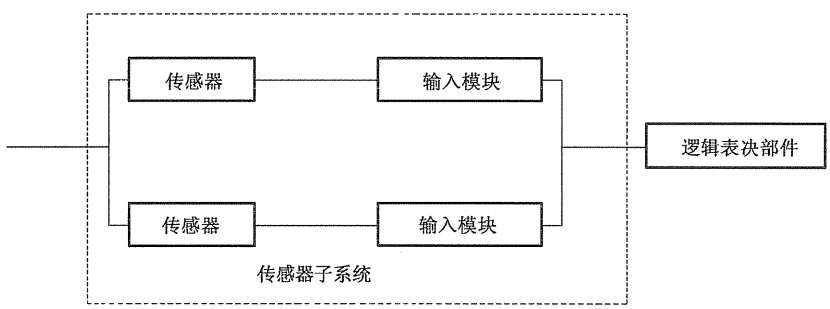


图 B.1 两个传感器通道配置示例

表 B.1　本附录中使用的术语及其范围(应用于 1oo1、1oo2、2oo2、1oo2D、2oo3)

缩略语及符号	术 语(单 位)	表 B.2～表 B.5 及 B.10～表 B.13 的参数范围
T_1	检验测试时间间隔(h)	1 个月(730 h)[a] 3 个月(2 190 h)[a] 6 个月(4 380 h) 1 年(8 760 h) 2 年(17 520 h)[b] 10 年(87 600 h)[b]
MTTR	平均恢复时间(h)	8 h
DC	诊断覆盖率(在公式中以一个分数或者百分比表示)	0% 60% 90% 99%
β	具有共同原因的、没有被检测到的失效分数(在公式中用一个分数或者百分比表示)(表 B.1～表 B.5 及表 B.10～表 B.13 中假设 $\beta=2\times\beta_D$)	2% 10% 20%
β_D	具有共同原因的、已被诊断测试检测到的失效分数(在公式中表示成一个分数或者百分比)(表 B.2～表 B.5 和表 B.10～表 B.13 中假设 $\beta=2\times\beta_D$)	1% 5% 10%
λ	子系统中一个通道的失效率(每小时)	0.1×10^{-6} 0.5×10^{-6} 1×10^{-6} 5×10^{-6} 10×10^{-6} 50×10^{-6}
PFD_G	表决通道组在要求时的平均失效概率(如果传感器、逻辑或最终元件子系统仅由一个表决组构成,则 PFD_G 分别等于 PFD_S、PFD_L 或 PFD_{FE})	
PFD_S	传感器子系统在要求时的平均失效概率	
PFD_L	逻辑子系统在要求时的平均失效概率	
PFD_{FE}	最终元件子系统在要求时的平均失效概率	
PFD_{SYS}	E/E/PE 安全相关系统的一个安全功能每小时的平均失效概率	
PFH_G	表决通道组在要求时的每小时平均失效概率(如果传感器、逻辑或最终元件子系统仅由一个表决组构成,则 PFD_G 分别等于 PFH_S、PFH_L 或 PFH_{FE})	
PFH_S	传感器子系统每小时的失效概率	

表 B.1（续）

缩略语及符号	术 语(单 位)	表 B.2～表 B.5 及 B.10～表 B.13 的参数范围
PFH_L	逻辑子系统每小时的失效概率	
PFH_{FE}	最终元件子系统每小时的失效概率	
PFH_{SYS}	E/E/PE 安全相关系统中安全功能每小时的平均失效概率	
λ_D	子系统中通道的危险失效率(每小时)，等于 0.5λ(假设 50%的危险失效和 50%的安全失效)	
λ_{DD}	检测到的子系统中通道每小时的危险失效率(它是在子系统通道中所有检测到的危险失效率的总和)	
λ_{DU}	未检测到的子系统中通道每小时的危险失效率(它是在子系统通道中所有未检测到的危险失效率的总和)	
λ_{SD}	子系统中被检测到的通道每小时的安全失效率(它是在子系统通道中所有检测到的安全失效率的总和)	
t_{CE}	1oo1、1oo2、2oo2、1oo2D、2oo3 结构中通道的等效平均停止工作时间(h)(它是子系统通道中所有部件的组合关闭时间)	
t_{GE}	1oo2、2oo3 结构中表决组的等效平均停止工作时间(h)(它是表决组中所有部件的组合关闭时间)	
t_{CE}'	1oo2D 结构中通道的等效平均停止工作时间(h)(它是子系统通道中所有部件的组合关闭时间)	
t_{GE}'	1oo2D 结构中表决组的等效平均停止工作时间(h)(它是表决组中所有部件的组合关闭时间)	
T_2	要求之间的时间间隔	

a 仅对于高要求或连续操作模式。

b 仅对于低要求操作模式。

B.2 要求的平均失效概率(对于低要求操作模式)

B.2.1 计算的过程

E/E/PE 安全相关系统的安全功能在要求时的平均失效概率，是通过计算和组合提供安全功能的所有子系统在要求时的平均失效概率确定的。因为在此附录中的失效概率很低，它可以表示为(见图 B.2)：

$$PFD_{SYS}=PFD_S+PFD_L+PFD_{FE}$$

式中：

PFD_{SYS}——E/E/PE 安全相关系统的安全功能在要求时的平均失效概率；

PFD_S——传感器子系统要求的平均失效概率；

PFD_L——逻辑子系统要求的平均失效概率；

PFD_{FE}——最终元件子系统要求的平均失效概率。

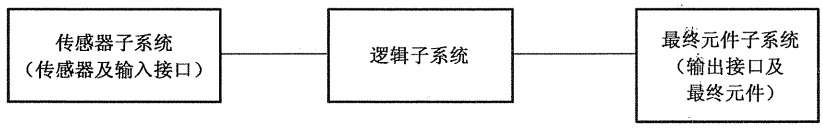


图 B.2　子系统结构

为了确定每一个子系统在要求时的平均失效概率，在子系统中应依次坚持下列步骤：

a) 画出表示传感器子系统(输入)各部件、逻辑子系统各部件、最终元件子系统(输出)各部件的块图。例如，传感器子系统的部件可能是传感器、屏蔽电路、输入调节电路；逻辑子系统部件可能是处理器和扫描设备；最终元件子系统部件可能是输出调节电路，屏蔽电路及执行器。将每一个子系统描绘成 1oo1、1oo2、2oo2、1oo2D、2oo3 表决组。

b) 参考相关的表 B.2～表 B.5，它们分别提供了 6 个月、1 年、2 年以及 10 年检验测试时间间隔的数据。这些表也假定了一旦失效被揭露出，则每次失效的平均恢复时间为 8 h。

c) 对于每一个子系统中的表决组要从表 B.2～表 B.5 中相关的表中选择：

——结构(例如 2oo3)；

——每个通道的诊断覆盖率(例如 60%)；

——每个通道的失效率(每小时)λ，(例如，5.0E-06)；

——表决组中通道之间相互作用的共同原因失效的 β 系数，β 和 β_D(例如分别为 2%和 1%)。

注 1：假设表决组中的每一个通道具有相同的诊断覆盖率和失效率(见 B.1)。

注 2：在表 B.2～表 B.5(以及表 B.10～表 B.13)中假设在不存在诊断测试时的 β 系数(也用于在诊断测试时未检测到的危险失效)β，是诊断测试检测到的失效的 β 系数的两倍，β_D。

d) 从表 B.2～表 B.5 中的相关表中获得表决组要求时的平均失效概率。

e) 如果安全功能依赖于传感器或执行器的多个表决组，传感器或最终元件子系统在要求时的组合平均失效概率 PFD_S 或 PFD_{FE} 已在下列式子中给出，其中 PFD_{Gi}、PFD_{Gj} 分别为传感器与最终元件的每个表决组在要求时的平均失效概率。

$$PFD_S = \sum_i PFD_{Gi}$$

$$PFD_{FE} = \sum_j PFD_{Gj}$$

B.2.2　低要求操作模式的结构

注 1：应按顺序阅读本条，因为对几种结构有效的公式仅在第一次使用时才被说明。

注 2：这些公式是基于表 B.1 的假设而得出的。

B.2.2.1　1oo1

这种结构包括一个单通道。在这种结构中当产生一次要求时，任何危险失效就会导致一个安全功能失效。

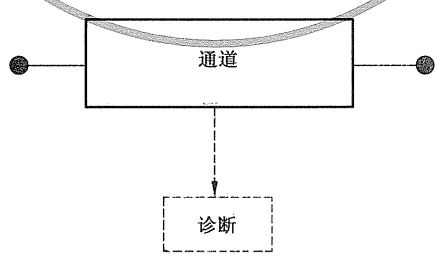


图 B.3　1oo1 物理块图

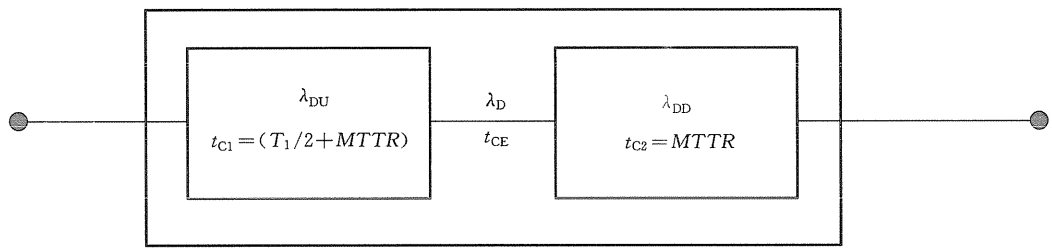


图 B.4　1oo1 可靠性块图

图 B.3 与图 B.4 包括了有关的块图，通道的危险失效率为：

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}$$

图 B.4 显示，通道可以被认为由两部分组成，其中一个具有由未被检测到的失效导致的危险失效率 λ_{DU}，另一部分具有由已被检测到的失效导致的危险失效率 λ_{DD}，通道的等效平均停止工作时间 t_{CE}，等于两部分各自的停止工作时间 t_{C1} 和 t_{C2} 相加，它与各部分对通道失效概率的贡献直接成比例：

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

对于每种结构，已被检测和未被检测到的危险失效率如下：

$$\lambda_{DU} = \frac{\lambda}{2}(1 - DC)\,;\lambda_{DD} = \frac{\lambda}{2} DC$$

对于一个具有由危险失效而导致关闭时间为 t_{CE} 的通道：

$$PFD = 1 - e^{\lambda_D t_{CE}}$$
$$\approx \lambda_D t_{CE}$$

因为 $\lambda_D t_{CE} \ll 1$

因此，对于 1oo1 结构，在要求时的平均失效概率为：

$$PFD_G = (\lambda_{DU} + \lambda_{DD})\ t_{CE}$$

B.2.2.2　1oo2

此结构由两个并联的通道构成，无论哪一个通道都能处理安全功能。因此，如果两个通道都存在危险失效，则在要求时某个安全功能失效。假设任何诊断测试仅报告发现故障，但并不改变任何输出状态或输出表决。

图 B.5 与图 B.6 中包含了相关的块图，t_{CE} 的值在 B.2.2.1 中已经给出，但是现在还需计算系统等效停止工作时间 t_{GE}，表示如下：

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DU}}{\lambda_D} MTTR$$

此结构在要求时的平均失效概率为：

$$PFD_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t'_{CE}t'_{GE} + \beta_D\lambda_{DD}MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

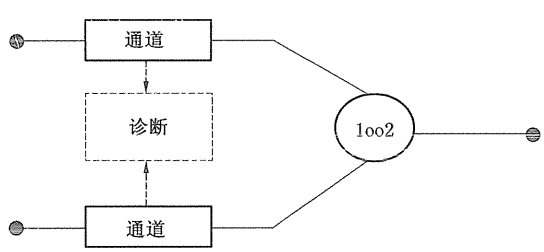


图 B.5　1oo2 物理块图

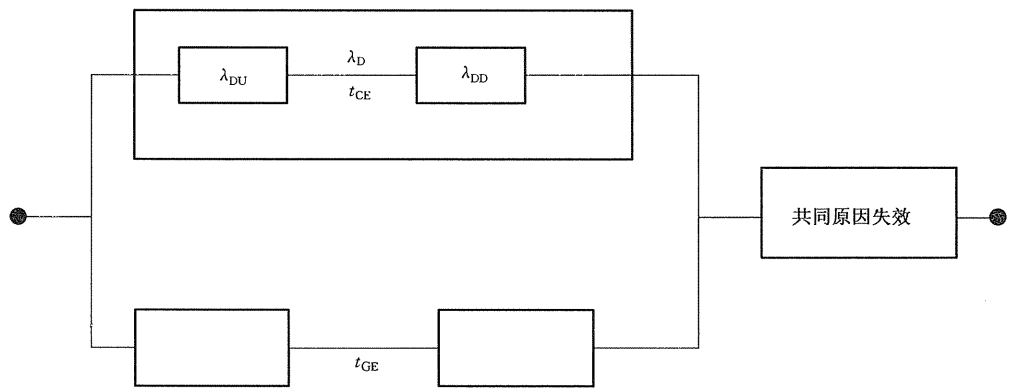


图 B.6　1oo2 可靠性块图

B.2.2.3　2oo2

此结构由并联的两个通道构成，因此，在发生安全功能之前两个通道都要求安全功能。假设任何诊断测试仅报告发现故障，并不改变任何输出状态或输出表决。

图 B.7 与图 B.8 包含了相关的块图，t_{CE}的值已在 B.2.2.1 中给出，此结构在要求时的平均失效概率如下：

$$PFD_G = 2\lambda_D t_{CE}$$

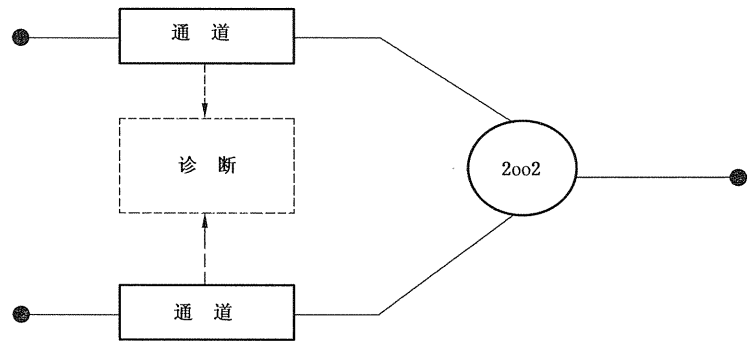


图 B.7　2oo2 物理块图

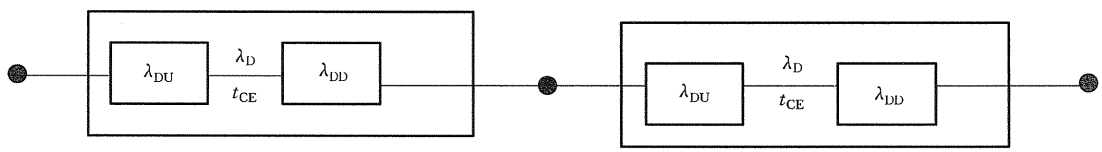


图 B.8　2oo2 可靠性块图

B.2.2.4　1oo2D

此结构中由并联的两个通道构成，正常工作期间，在发生安全功能之前，两个通道都要求安全功能。此外，如果任一通道中诊断测试检测到一个故障，则将采用输出表决，因此整个输出状态则按照另一通道给出的输出状态。如果诊断测试在两个通道同时检测到故障，或者检测到两个通道间存在的差异时，输出则转到安全状态。为了检测两个通道间的差异，通过一种与另一通道无关的方法，无论其中哪个通道都能确定另一通道的状态。

每个通道中被检测的安全失效率如下：

$$\lambda_{SD} = \lambda/2DC$$

图 B.9 与图 B.10 包含相关的块图，B.2.2 中的等效平均停止工作时间的值与其他结构给出的数值不同，因此它们被表示为 t'_{CE} 与 t'_{GE}：

$$t'_{CE}=[\lambda_{DU}/(T_1/2+MTTR)+(\lambda_{DD}+\lambda_{SD})MTTR]/(\lambda_{DU}+\lambda_{DD}+\lambda_{SD})$$

$$t'_{GE}=[\lambda_{DU}(T_1/3+MTTR)+(\lambda_{DD}+\lambda_{SD})MTTR]/(\lambda_{DU}+\lambda_{DD}+\lambda_{SD})$$

结构在要求时的平均失效概率如下：

$$PFD_G=2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU})+(1-\beta_D)\lambda_{DD}+\lambda_{SD})t'_{CE}t'_{GE}+\beta_D\lambda_{DD}MTTR+\beta\lambda_{DU}(T_1/2+MTTR)$$

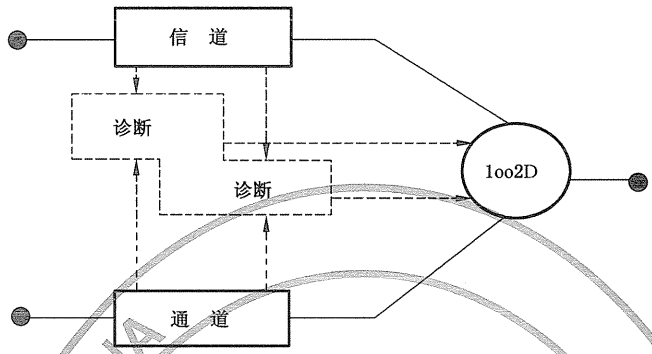


图 B.9 1oo2D 物理块图

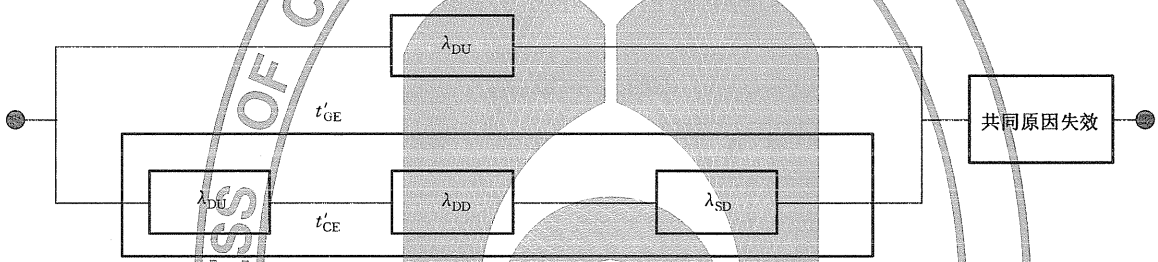


图 B.10 1oo2D 可靠性块图

B.2.2.5 2oo3

此结构由 3 个并联通道构成，其输出信号具有多数表决安排，这样，如果仅其中一个通道的输出与其他两个通道的输出状态不同时，输出状态不会因此而改变。假设任何诊断测试只报告发现故障，不改变任何输出状态或者输出表决。

图 B.11 与图 B.12 包含了相关的块图。t_{CE}的值同 B.2.2.1 中给出的值相同，t_{GE}的值同 B.2.2.2 中给出的值相同。在要求时结构的平均失效概率为：

$$PFD_G=6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})^2t_{CE}t_{GE}+\beta_D\lambda_{DD}MTTR+\beta\lambda_{DU}(T_1/2+MTTR)$$

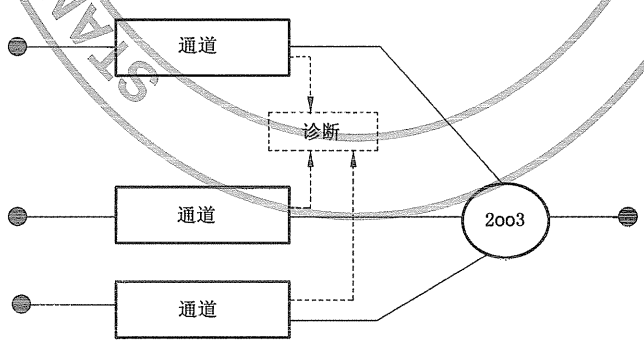


图 B.11 2oo3 物理块图

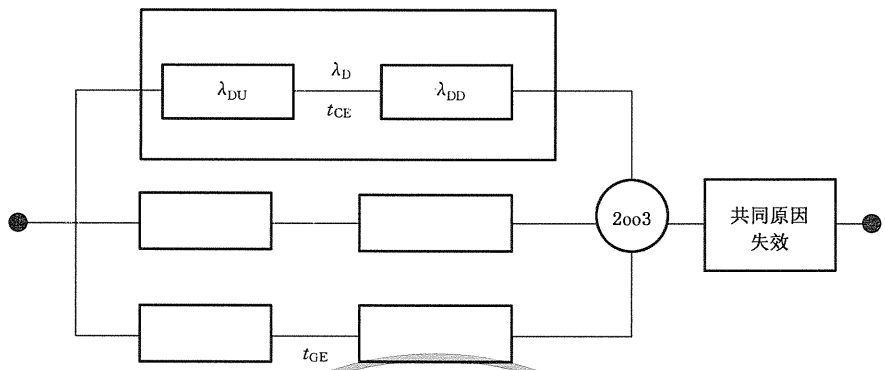


图 B.12　2oo3 可靠性块图

B.2.3　低要求操作模式的详表(表 B.2～表 B.5)

表 B.2　检验测试时间间隔为 6 个月、平均恢复时间 8 h 时要求的平均失效概率

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1 (见注 2)	0%	1.1E-04			5.5E-04			1.1E-03		
	60%	4.4E-05			2.2E-04			4.4E-04		
	90%	1.1E-05			5.7E-05			1.1E-04		
	99%	1.5E-06			7.5E-06			1.5E-05		
1oo2	0%	2.2E-06	1.1E-05	2.2E-05	1.1E-05	5.5E-05	1.1E-04	2.4E-05	1.1E-04	2.2E-04
	60%	8.8E-07	4.4E-06	8.8E-06	4.5E-06	2.2E-05	4.4E-05	9.1E-06	4.4E-05	8.8E-05
	90%	2.2E-07	1.1E-06	2.2E-06	1.1E-06	5.6E-06	1.1E-05	2.3E-06	1.1E-05	2.2E-05
	99%	2.2E-08	1.3E-07	2.6E-07	1.3E-07	6.5E-07	1.3E-06	2.6E-07	1.3E-06	2.6E-06
2oo2 (见注 2)	0%	2.2E-04			1.1E-03			2.2E-03		
	60%	8.8E-05			4.4E-04			8.8E-04		
	90%	2.3E-05			1.1E-04			2.3E-04		
	99%	3.0E-06			1.5E-05			3.0E-05		
1oo2D	0%	2.2E-06	1.1E-05	2.2E-05	1.1E-05	5.5E-05	1.1E-04	2.4E-05	1.1E-04	2.2E-04
	60%	8.8E-07	4.4E-06	8.8E-06	4.5E-06	2.2E-05	4.4E-05	8.9E-06	4.4E-05	8.8E-05
	90%	2.2E-07	1.1E-06	2.2E-06	1.1E-06	5.6E-06	1.1E-05	2.2E-06	1.1E-05	2.2E-05
	99%	2.6E-08	1.3E-07	2.6E-07	1.3E-07	6.5E-07	1.3E-06	2.6E-07	1.3E-06	2.6E-06
2oo3	0%	2.2E-06	1.1E-05	2.2E-05	1.1E-05	5.6E-05	1.1E-04	2.7E-05	1.1E-04	2.2E-04
	60%	8.9E-07	4.4E-06	8.8E-06	4.6E-06	2.2E-05	4.4E-05	9.6E-06	4.5E-05	8.9E-05
	90%	2.2E-07	1.1E-06	2.2E-06	1.1E-06	5.6E-06	1.1E-05	2.3E-06	1.1E-05	2.2E-05
	99%	2.6E-08	1.3E-07	2.6E-07	1.3E-07	6.5E-07	1.3E-06	2.6E-07	1.3E-06	2.6E-06

表 B.2（续）

结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1（见注 2）	0%	5.5E-03			1.1E-02			5.5E-02		
	60%	2.2E-03			4.4E-03			2.2E-02		
	90%	5.7E-04			1.1E-03			5.7E-03		
	99%	7.5E-05			1.5E-04			7.5E-04		
1oo2	0%	1.5E-04	5.8E-04	1.1E-03	3.7E-04	1.2E-03	2.3E-03	5.0E-03	8.8E-03	1.4E-02
	60%	5.0E-05	2.3E-04	4.5E-04	1.1E-04	4.6E-04	9.0E-04	1.1E-03	2.8E-03	4.9E-03
	90%	1.2E-05	5.6E-05	1.1E-04	2.4E-05	1.1E-04	2.2E-04	1.5E-04	6.0E-04	1.2E-03
	99%	1.3E-06	6.5E-06	1.3E-05	2.6E-06	1.3E-05	2.6E-05	1.4E-05	6.6E-05	1.3E-04
2oo2（见注 2）	0%	1.1E-02			2.2E-02			>1.0E-01		
	60%	4.4E-03			8.8E-03			4.4E-02		
	90%	1.1E-03			2.3E-03			1.1E-02		
	99%	1.5E-04			3.0E-04			1.5E-03		
1oo2D	0%	1.5E-04	5.8E-04	1.1E-03	3.7E-04	1.2E-03	2.3E-03	5.0E-03	8.8E-03	1.4E-02
	60%	4.6E-05	2.2E-04	4.4E-04	9.5E-05	4.5E-04	8.9E-04	6.0E-04	2.3E-03	4.5E-03
	90%	1.1E-05	5.6E-05	1.1E-04	2.2E-05	1.1E-04	2.2E-04	1.1E-04	5.6E-04	1.1E-03
	99%	1.3E-06	6.5E-06	1.3E-05	2.6E-06	1.3E-05	2.6E-05	1.3E-05	6.5E-05	1.3E-04
2oo3	0%	2.3E-04	6.5E-04	1.2E-03	6.8E-04	1.5E-03	2.5E-03	1.3E-02	1.5E-02	1.9E-02
	60%	6.3E-05	2.4E-04	4.6E-04	1.6E-04	5.1E-04	9.4E-04	2.3E-03	3.9E-03	5.9E-03
	90%	1.2E-05	5.7E-05	1.1E-04	2.7E-05	1.2E-04	2.3E-04	2.4E-04	6.8E-04	1.2E-03
	99%	1.3E-06	6.5E-06	1.3E-05	2.7E-06	1.3E-05	2.6E-05	1.5E-05	6.7E-05	1.3E-04

注 1：此表给出了 PFD_G 的示例值，它是根据 B.1 中所列出的假设，使用 B.2.2 中的公式计算出的，如果传感器、逻辑元件、最终元件子系统仅由一个表决通道组构成，那么 PFD_G 分别与 PFD_S、PFD_L 或 PFD_{FE} 的数值相等（见 B.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均失效概率。

表 B.3 检验测试时间间隔为 1 年、平均恢复时间为 8 h 时要求的平均失效概率

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1（见注 2）	0%	2.2E-04			1.1E-03			2.2E-03		
	60%	8.8E-05			4.4E-04			8.8E-04		
	90%	2.2E-05			1.1E-04			2.2E-04		
	99%	2.6E-06			1.3E-05			2.6E-05		

表 B.3（续）

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo2	0%	4.4E-06	2.2E-05	4.4E-05	2.3E-05	1.1E-04	2.2E-04	5.0E-05	2.2E-04	4.4E-04
	60%	1.8E-06	8.8E-06	1.8E-05	9.0E-06	4.4E-05	8.8E-05	1.9E-05	8.9E-05	1.8E-04
	90%	4.4E-07	2.2E-06	4.4E-06	2.2E-06	1.1E-05	2.2E-05	4.5E-06	2.2E-05	4.4E-05
	99%	4.8E-08	2.4E-07	4.8E-07	2.4E-07	1.2E-06	2.4E-06	4.8E-07	2.4E-06	4.8E-06
2oo2（见注 2）	0%	4.4E-04			2.2E-03			4.4E-03		
	60%	1.8E-04			8.8E-04			1.8E-03		
	90%	4.5E-05			2.2E-04			4.5E-04		
	99%	5.2E-06			2.6E-05			5.2E-05		
1oo2D	0%	4.4E-06	2.2E-05	4.4E-05	2.3E-05	1.1E-04	2.2E-04	5.0E-05	2.2E-04	4.4E-04
	60%	1.8E-06	8.8E-06	1.8E-05	8.9E-06	4.4E-05	8.8E-05	1.8E-05	8.8E-05	1.8E-04
	90%	4.4E-07	2.2E-06	4.4E-06	2.2E-06	1.1E-05	2.2E-05	4.4E-06	2.2E-05	4.4E-05
	99%	4.8E-08	2.4E-07	4.8E-07	2.4E-07	1.2E-06	2.4E-06	4.8E-07	2.4E-06	4.8E-06
2oo3	0%	4.6E-06	2.2E-05	4.4E-05	2.7E-05	1.1E-04	2.2E-04	6.2E-05	2.4E-04	4.5E-04
	60%	1.8E-06	8.8E-06	1.8E-06	9.5E-06	4.5E-05	8.8E-05	2.1E-05	9.1E-05	1.8E-04
	90%	4.4E-07	2.2E-06	4.4E-06	2.3E-06	1.1E-05	2.2E-05	4.6E-06	2.2E-05	4.4E-05
	99%	4.8E-08	2.4E-07	4.8E-07	2.4E-07	1.2E-06	2.4E-06	4.8E-07	2.4E-06	4.8E-06
结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1（见注 2）	0%	1.1E-02			2.2E-02			>1.0E-01		
	60%	4.4E-03			8.8E-03			4.4E-02		
	90%	1.1E-03			2.2E-03			1.1E-02		
	99%	1.3E-04			2.6E-04			1.3E-03		
1oo2	0%	3.7E-04	1.2E-03	2.3E-03	1.1E-03	2.7E-03	4.8E-03	1.8E-02	2.4E-02	3.2E-02
	60%	1.1E-05	4.6E-04	9.0E-04	2.8E-04	9.7E-04	1.8E-03	3.4E-03	6.6E-03	1.1E-02
	90%	2.4E-05	1.1E-04	2.2E-04	5.1E-05	2.3E-04	4.5E-04	3.8E-04	1.3E-03	2.3E-03
	99%	2.4E-06	1.2E-05	2.4E-05	4.9E-06	2.4E-05	4.8E-05	2.6E-05	1.2E-04	2.4E-04
2oo2（见注 2）	0%	2.2E-02			4.4E-02			>1.0E-01		
	60%	8.8E-03			1.8E-02			8.8E-02		
	90%	2.2E-03			4.5E-03			2.2E-02		
	99%	2.6E-04			5.2E-04			2.6E-03		

表 B.3（续）

结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo2D	0%	3.7E-04	1.2E-03	2.3E-03	1.1E-03	2.7E-03	4.8E-03	1.8E-02	2.4E-02	3.2E-02
	60%	9.4E-05	4.5E-04	8.8E-04	2.0E-04	9.0E-04	1.8E-03	1.5E-03	5.0E-03	9.3E-03
	90%	2.2E-05	1.1E-04	2.2E-04	4.5E-05	2.2E-04	4.4E-04	2.3E-04	1.1E-03	2.2E-03
	99%	2.4E-06	1.2E-05	2.4E-05	4.8E-06	2.4E-05	4.8E-05	2.4E-05	1.2E-04	2.4E-04
2oo3	0%	6.8E-04	1.5E-03	2.5E-03	2.3E-03	3.8E-03	5.6E-03	4.8E-02	5.0E-02	5.3E-02
	60%	1.6E-04	5.1E-04	9.4E-04	4.8E-04	1.1E-03	2.0E-03	8.4E-03	1.1E-02	1.5E-02
	90%	2.7E-05	1.2E-04	2.3E-04	6.4E-05	2.4E-04	4.6E-04	7.1E-04	1.6E-03	2.6E-03
	99%	2.5E-06	1.2E-05	2.4E-05	5.1E-06	2.4E-05	4.8E-05	3.1E-05	1.3E-04	2.5E-04

注 1：此表给出了 PFD_G 的示例值，它是根据 B.1 中所列出的假设，使用 B.2.2 中的公式计算出的，如果传感器、逻辑元件、最终元件子系统仅由一个表决通道组构成，那么 PFD_G 分别与 PFD_S、PFD_L 或 PFD_{FE} 的数值相等（见 B.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均失效概率。

表 B.4 检验测试时间间隔为 2 年、平均恢复时间为 8 h 时要求的平均失效概率

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1（见注 2）	0%	4.4E-04			2.2E-03			4.4E-03		
	60%	1.8E-04			8.8E-04			1.8E-03		
	90%	4.4E-05			2.2E-04			4.4E-04		
	99%	4.8E-06			2.4E-05			4.8E-05		
1oo2	0%	9.0E-06	8.8E-05	8.8E-05	5.0E-05	2.2E-04	4.4E-04	1.1E-04	4.6E-04	8.9E-04
	60%	3.5E-06	1.8E-05	3.5E-05	1.9E-05	8.9E-05	1.8E-04	3.9E-05	1.8E-04	3.5E-04
	90%	8.8E-07	4.4E-06	8.8E-06	4.5E-06	2.2E-05	4.4E-05	9.1E-06	4.4E-05	8.8E-05
	99%	9.2E-08	4.6E-07	9.2E-07	4.6E-07	2.3E-06	4.6E-06	9.2E-07	4.6E-06	9.2E-06
2oo2（见注 2）	0%	8.8E-04			4.4E-03			8.8E-03		
	60%	3.5E-04			1.8E-03			3.5E-03		
	90%	8.8E-05			4.4E-04			8.8E-04		
	99%	9.6E-06			4.8E-05			9.6E-05		
1oo2D	0%	9.0E-06	4.4E-05	8.8E-05	5.0E-05	2.2E-04	4.4E-04	1.1E-04	4.6E-04	8.9E-04
	60%	3.5E-06	1.8E-05	3.5E-05	1.9E-05	8.9E-05	1.8E-04	3.9E-05	1.8E-04	3.5E-04
	90%	8.8E-07	4.4E-06	8.8E-06	4.5E-06	2.2E-05	4.4E-05	9.1E-06	4.4E-05	8.8E-05
	99%	9.2E-08	4.6E-07	9.2E-07	4.6E-07	2.3E-06	4.6E-06	9.2E-07	4.6E-06	9.2E-06

表 B.4（续）

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
2oo3	0%	9.5E-06	4.4E-05	8.8E-05	6.2E-05	2.3E-04	4.5E-04	1.6E-04	5.0E-04	9.3E-04
	60%	3.6E-06	1.8E-05	3.5E-05	2.1E-05	9.0E-05	1.8E-04	4.7E-05	1.9E-04	3.6E-04
	90%	8.9E-07	4.4E-06	8.8E-06	4.6E-06	2.2E-05	4.4E-05	9.6E-06	4.5E-05	8.9E-05
	99%	9.2E-08	4.6E-07	9.2E-07	4.6E-07	2.3E-06	4.6E-06	9.3E-07	4.6E-06	9.2E-06
结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1（见注 2）	0%	2.2E-02			4.4E-02			>1.0E-01		
	60%	8.8E-03			1.8E-02			8.8E-02		
	90%	2.2E-03			4.4E-03			2.2E-02		
	99%	2.4E-04			4.8E-04			2.4E-03		
1oo2	0%	1.1E-03	2.7E-03	4.8E-03	3.3E-03	6.5E-03	1.0E-02	6.6E-02	7.4E-02	8.5E-02
	60%	2.8E-04	9.7E-04	1.8E-03	7.5E-04	2.1E-03	3.8E-03	1.2E-02	1.8E-02	2.5E-02
	90%	5.0E-05	2.3E-04	4.5E-04	1.1E-04	4.6E-04	9.0E-04	1.1E-03	2.8E-03	4.9E-03
	99%	4.7E-06	2.3E-05	4.6E-05	9.5E-06	4.6E-05	9.2E-05	5.4E-05	2.4E-04	4.6E-04
2oo2（见注 2）	0%	4.4E-02			8.8E-02			>1.0E-01		
	60%	1.8E-02			3.5E-02			>1.0E-01		
	90%	4.4E-03			8.8E-03			4.4E-02		
	99%	4.8E-04			9.6E-04			4.8E-03		
1oo2D	0%	1.1E-03	2.7E-03	4.8E-03	3.3E-03	6.5E-03	1.0E-02	6.6E-02	7.4E-02	8.5E-02
	60%	2.0E-04	9.0E-04	1.8E-03	4.5E-04	1.8E-03	3.6E-03	4.3E-03	1.1E-02	1.9E-02
	90%	4.4E-05	2.2E-04	4.4E-04	8.9E-05	4.4E-04	8.8E-04	4.7E-04	2.2E-03	4.4E-03
	99%	4.6E-06	2.3E-05	4.6E-05	9.2E-06	4.6E-05	9.2E-05	4.6E-05	2.3E-04	4.6E-04
2oo3	0%	2.3E-03	3.7E-03	5.6E-03	8.3E-03	1.1E-02	1.4E-02	>1.0E-01	>1.0E-01	>1.0E-01
	60%	4.8E-04	1.1E-04	2.0E-03	1.6E-04	2.8E-03	4.4E-03	3.2E-02	3.5E-02	4.0E-02
	90%	6.3E-05	2.4E-04	4.6E-04	1.6E-04	5.1E-04	9.4E-04	2.4E-03	4.0E-03	6.0E-03
	99%	4.8E-06	2.3E-05	4.6E-05	1.0E-06	4.7E-05	9.2E-05	6.9E-05	2.5E-04	4.8E-04

注 1：此表给出了 PFD_G 的示例值，它是根据 B.1 中所列出的假设，使用 B.2.2 中的公式计算出的，如果传感器、逻辑元件、最终元件子系统仅由一个表决通道组构成，那么 PFD_G 分别与 PFD_S、PFD_L 或 PFD_{FE} 的数值相等（见 B.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均失效概率。

表 B.5　检验测试时间间隔为 10 年、平均恢复时间为 8 h 时要求的平均失效概率

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1 （见注 2）	0%	2.2E-03			1.1E-02			2.2E-02		
	60%	8.8E-04			4.4E-03			8.8E-03		
	90%	2.2E-04			1.1E-03			2.2E-03		
	99%	2.2E-05			1.1E-04			2.2E-04		
1oo2	0%	5.0E-05	2.2E-04	4.4E-04	3.7E-04	1.2E-03	2.3E-03	1.1E-03	2.7E-03	4.8E-03
	60%	1.9E-05	8.9E-05	1.8E-04	1.1E-04	4.6E-04	9.0E-04	2.7E-04	9.6E-04	1.8E-03
	90%	4.4E-06	2.2E-05	4.4E-05	2.3E-05	1.1E-04	2.2E-04	5.0E-05	2.2E-04	4.4E-04
	99%	4.4E-07	2.2E-06	4.4E-06	2.2E-06	1.1E-05	2.2E-05	4.5E-06	2.2E-05	4.4E-05
2oo2 （见注 2）	0%	4.4E-03			2.2E-02			4.4E-02		
	60%	1.8E-03			8.8E-03			1.8E-02		
	90%	4.4E-04			2.2E-03			4.4E-03		
	99%	4.5E-05			2.2E-04			4.5E-04		
1oo2D	0%	5.0E-05	2.2E-04	4.4E-04	3.7E-04	1.2E-03	2.3E-03	1.1E-03	2.7E-03	4.8E-03
	60%	1.8E-05	8.9E-05	1.8E-04	9.4E-05	4.4E-04	8.8E-04	2.0E-04	9.0E-04	1.8E-03
	90%	4.4E-06	2.2E-05	4.4E-05	2.3E-05	1.1E-04	2.2E-04	4.4E-05	2.2E-04	4.4E-04
	99%	4.4E-07	2.2E-06	4.4E-06	2.2E-06	1.1E-05	2.2E-05	4.4E-06	2.2E-05	4.4E-05
2oo3	0%	6.2E-05	2.3E-04	4.5E-04	6.8E-04	1.5E-03	2.5E-03	2.3E-03	3.7E-03	5.6E-03
	60%	2.1E-05	9.0E-05	1.8E-04	1.6E-04	5.0E-04	9.3E-04	4.7E-04	1.1E-03	2.0E-03
	90%	4.6E-06	2.2E-05	4.4E-05	2.7E-05	1.1E-04	2.2E-04	6.3E-05	2.4E-04	4.5E-04
	99%	4.4E-07	2.2E-06	4.4E-06	2.3E-06	1.1E-05	2.2E-05	4.6E-06	2.2E-05	4.4E-05
结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1 （见注 2）	0%	>1.0E-01			>1.0E-01			>1.0E-01		
	60%	4.4E-02			8.8E-02			>1.0E-01		
	90%	1.1E-02			2.2E-02			>1.0E-01		
	99%	1.1E-03			2.2E-03			1.1E-02		
1oo2	0%	1.8E-02	2.4E-02	3.2E-02	6.6E-02	7.4E-02	8.5E-02	>1.0E-01	>1.0E-01	>1.0E-01
	60%	3.4E-03	6.6E-03	1.1E-02	1.2E-02	1.8E-02	2.5E-02	>1.0E-01	>1.0E-01	>1.0E-01
	90%	3.8E-04	1.2E-03	2.3E-03	1.1E-03	2.8E-03	4.9E-03	1.8E-02	2.5E-02	3.5E-02
	99%	2.4E-05	1.1E-04	2.2E-04	5.1E-05	2.3E-04	4.5E-04	3.8E-04	1.3E-03	2.3E-03
2oo2 （见注 2）	0%	>1.0E-01			>1.0E-01			>1.0E-01		
	60%	8.8E-02			>1.0E-01			>1.0E-01		
	90%	2.2E-02			4.4E-02			>1.0E-01		
	99%	2.2E-03			4.5E-03			2.2E-02		

表 B.5（续）

结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo2D	0%	1.8E-02	2.4E-02	3.2E-02	6.6E-02	7.4E-02	8.5E-02	>1.0E-01	>1.0E-01	>1.0E-01
	60%	1.5E-03	4.9E-03	9.2E-03	4.2E-03	1.1E-02	1.9E-02	7.1E-02	9.9E-02	>1.0E-01
	90%	2.3E-04	1.1E-03	2.2E-03	4.7E-04	2.2E-03	4.4E-03	3.0E-03	1.2E-02	2.3E-02
	99%	2.2E-05	1.1E-04	2.2E-04	4.4E-05	2.2E-04	4.4E-04	2.2E-04	1.1E-03	2.2E-03
2oo3	0%	4.8E-02	5.0E-02	5.3E-02	>1.0E-01	>1.0E-01	>1.0E-01	>1.0E-01	>1.0E-01	>1.0E-01
	60%	8.3E-03	1.1E-02	1.4E-02	3.2E-02	3.5E-02	4.0E-02	>1.0E-01	>1.0E-01	>1.0E-01
	90%	6.9E-04	1.5E-03	2.6E-03	2.3E-03	3.9E-03	5.9E-03	4.9E-02	5.4E-02	6.0E-02
	99%	2.7E-05	1.2E-04	2.3E-04	6.4E-05	2.4E-04	4.6E-04	7.1E-04	1.6E-03	2.6E-03

注 1：此表给出了 PFD_G 的示例值，它是根据 B.1 中所列出的假设，使用 B.2.2 中的公式计算出的，如果传感器、逻辑元件、最终元件子系统仅由一个表决通道组构成，那么 PFD_G 分别与 PFD_S、PFD_L 或 PFD_{FE} 的数值相等（见 B.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均失效概率。

B.2.4 低要求操作模式示例

考虑需要一个 SIL2 系统的安全功能。假设按前面的作法对系统结构的初始评估是，针对 1 组 3 个模拟压力传感器结构为表决 2oo3。逻辑子系统是配置为冗余 1oo2D 的 PES，用于驱动 1 个停机阀和 1 个通风阀。为了达到安全功能，需要操作通风阀和停机阀。在图 B.13 中显示了该系统的结构。初始评估时假设检验测试时间间隔为 1 年。

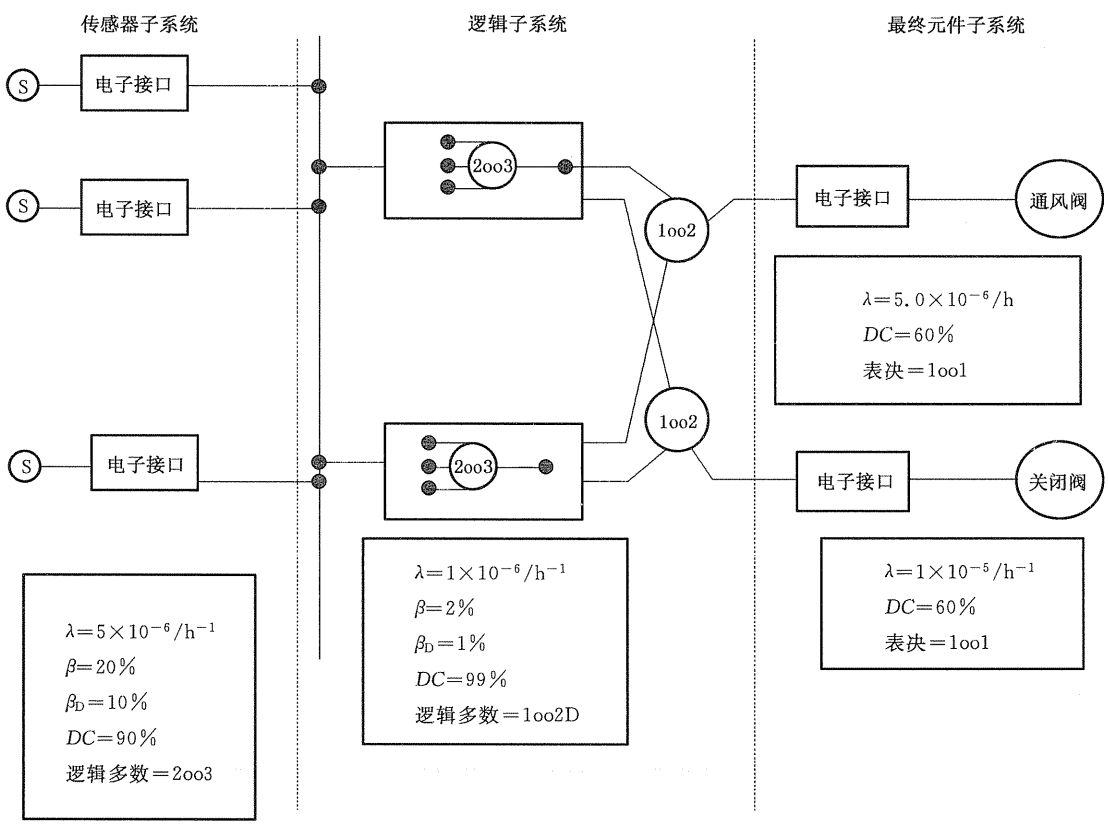


图 B.13 低要求操作模式结构示例

表 B.6 低要求操作模式示例中传感器子系统在要求时的平均失效概率
（检验测试时间间隔为 1 年，*MTTR* 为 8 h）

结构	*DC*	λ=5.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
2oo3	0%	6.8E-04	1.5E-03	2.5E-03
	60%	1.6E-04	5.1E-04	9.4E-04
	90%	2.7E-05	1.2E-04	2.3E-04
	99%	2.5E-06	1.2E-05	2.4E-05
注：此表摘自表 B.3。				

表 B.7 低要求操作模式示例中逻辑子系统在要求时的平均失效概率
（检验测试时间间隔为 1 年，*MTTR* 为 8 h）

结构	*DC*	λ=1.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo2D	0%	1.1E-03	2.7E-03	4.8E-03
	60%	2.0E-04	9.0E-04	1.8E-03
	90%	4.5E-05	2.2E-04	4.4E-04
	99%	4.8E-06	2.4E-05	4.8E-05
注：此表摘自表 B.3。				

表 B.8 低要求操作模式示例中最终元件子系统在要求时的平均失效概率
（检验测试时间间隔为 1 年，*MTTR* 为 8 h）

结构	*DC*	λ=5.0E-06	λ=1.0E-05
1oo1	0%	1.1E-02	2.2E-02
	60%	4.4E-03	8.8E-03
	90%	1.1E-03	2.2E-03
	99%	1.3E-04	2.6E-04
注：此表摘自表 B.3。			

从表 B.6～表 B.8 中可导出下列值：

对于传感器子系统：

$$PFD_S = 2.3 \times 10^{-4}$$

对于逻辑子系统：

$$PFD_L = 4.8 \times 10^{-6}$$

对于最终元件子系统：

$$PFD_{FE} = 4.4 \times 10^{-3} + 8.8 \times 10^{-3}$$
$$= 1.3 \times 10^{-2}$$

因此，对于安全功能：

$$PFD_{SYS} = 2.3\times10^{-4} + 4.8\times10^{-6} + 1.3\times10^{-2}$$
$$= 1.3\times10^{-2}$$
$$\equiv \text{安全完整性等级 1}$$

为了改进系统使其更好地适应安全完整性等级 2，需要完成下列工作之一：

a) 将检验测试的时间间隔改为 6 个月：

$PFD_S = 1.1\times10^{-4}$

$PFD_L = 2.6\times10^{-6}$

$PFD_{FE} = 2.2\times10^{-3} + 4.4\times10^{-4}$
$= 6.6\times10^{-3}$

$PFD_{SYS} = 6.7\times10^{-3}$
$\equiv$安全完整性等级 2

b) 1oo1 停机阀(其输出设备的可靠性较低)改为 1oo2(假设 β 值为 10%，β_D 值为 5%)

$PFD_S = 2.3\times10^{-4}$

$PFD_L = 4.8\times10^{-6}$

$PFD_{FE} = 4.4\times10^{-3} + 9.7\times10^{-4}$
$= 5.4\times10^{-3}$

$PFD_{SYS} = 5.6\times10^{-3}$
$\equiv$安全完整性等级 2

B.2.5 不完善检验测试的效应

在安全相关系统中的故障，既没有被诊断测试又没有被检验测试检测到，而仅由受故障影响而要求安全功能时才能被发现。因此，对这些完全检测不到的故障，安全相关系统预计的要求率决定了有效的停止工作时间。

下面给出了 1oo2 结构的例子，T_2 为向系统提要求的间隔时间。

$$t_{CE} = \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_2}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$t_{GE} = \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_2}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$PFD_G = 2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} t_{GE} + \beta_D\lambda_{DD}MTTR + \beta\frac{\lambda_{DU}}{2}\left(\frac{T_1}{2} + MTTR\right) + \beta\frac{\lambda_{DU}}{2}\left(\frac{T_2}{2} + MTTR\right)$$

表 B.9 给出了 1oo2 系统在时间间隔为期一年的情况下 100%的检验测试与 50%的检验测试对比的数字结果，其中要求时间间隔周期假设为 10 年。此例在计算中还假设失效率为 1×10^{-5}/h，其中 β 为 10%，β_D 为 5%。

表 B.9 不完善检验测试的示例

结构	DC	λ=1.0E-05	
		100%检验测试 β=10% β_D=5%	50%检验测试(T_2=10 年) β=10% β_D=5%
1oo2	0%	2.7E-03	6.6E-02
	60%	9.7E-04	2.6E-02
	90%	2.3E-04	6.6E-03
	99%	2.4E-05	7.0E-04

B.3 每小时的失效概率(对于高要求或连续操作模式)

B.3.1 计算的过程

高要求或连续操作模式下工作的 E/E/PE 安全相关系统的功能安全的失效概率的计算方法同对于低要求操作模式的计算方法相同(见 B.2.1),只是用每小时的危险失效概率(PFH_{SYS})代替要求时的平均失效概率(PFD_{SYS})。

E/E/PE 安全相关系统中安全功能的总危险失效概率 PFH_{SYS},是通过计算共同提供安全功能的所有子系统的危险失效概率,并把这些值相加得出。因为在此附录中的失效概率都很小,所以可表示如下:

$$PFH_{SYS}=PFH_S+PFH_L+PFH_{FE}$$

其中:

PFH_{SYS}——E/E/PE 安全相关系统的安全功能每小时的失效概率;

PFH_S——传感器子系统每小时的失效概率;

PFH_L——逻辑子系统每小时的失效概率;

PFH_{FE}——最终元件子系统每小时的失效概率。

B.3.2 高要求或连续操作模式的结构

注 1:本条应按顺序阅读,因为对几种结构有效的公式只在第一次使用时才有说明。另见 B.2.2。

注 2:计算基于表 B.1 中的假设。

B.3.2.1 1oo1

图 B.3 与图 B.4 显示了相关的块图。

$$\lambda_D=\lambda_{DU}+\lambda_{DD}=\frac{\lambda}{2}$$

$$t_{CE}=\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MTTR\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$\lambda_{DU}=\frac{\lambda}{2}(1-DC);\lambda_{DD}=\frac{\lambda}{2}DC$$

如果假设在检测到任何失效时安全相关系统将使 EUC 进入某种安全状态,对于 1oo1 结构,则可以得到如下公式:

$$PFH_G=\lambda_{DU}$$

B.3.2.2 1oo2

图 B.5 与图 B.6 显示了相关的块图。t_{CE}为 B.3.2.1 中给出的值。

$$PFH_G=2((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})^2t_{CE}+\beta_D\lambda_{DD}+\beta\lambda_{DU}$$

B.3.2.3 2oo2

图 B.7 与图 B.8 显示了相关的块图。如果假设在检测到任何失效时每个通道均进入某种安全状态,对于 2oo2 结构,则可以得到如下公式:

$$PFH_G=2\lambda_{DU}$$

B.3.2.4 1oo2D

图 B.9 与图 B.10 显示了相关的块图。

$$\lambda_{SD}=\frac{\lambda}{2}DC$$

$$t_{CE}=\frac{\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)+(\lambda_{DD}+\lambda_{SD})MTTR}{\lambda_{DU}+\lambda_{DD}+\lambda_{SD}}$$

$$PFH_G = 2(1-\beta)\ \lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})\ t'_{CE} + \beta_D\lambda_{DD} + \beta\lambda_{DU}$$

B.3.2.5 2oo3

图 B.11 与图 B.12 显示了相关的块图。t_{CE}为 B.3.2.1 中的值。

$$PFH_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} + \beta_D\lambda_{DD} + \beta\lambda_{DU}$$

B.3.3 高要求或连续操作模式的详表(表 B.10～表 B.13)

表 B.10 检验测试时间间隔为 1 个月,平均恢复时间为 8 h 时每小时的平均失效概率

(高要求或连续操作模式下)

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1 (见注 2)	0%	5.0E-08			2.5E-07			5.0E-07		
	60%	2.0E-08			1.0E-07			2.0E-07		
	90%	5.0E-09			2.5E-08			5.0E-08		
	99%	5.0E-10			2.5E-09			5.0E-09		
1oo2	0%	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60%	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.0E-09	3.5E-08	7.0E-08
	90%	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo2 (见注 2)	0%	1.0E-07			5.0E-07			1.0E-06		
	60%	4.0E-08			2.0E-07			4.0E-07		
	90%	1.0E-08			5.0E-08			1.0E-07		
	99%	1.0E-09			5.0E-09			1.0E-08		
1oo2D	0%	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60%	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.0E-09	3.5E-08	7.0E-08
	90%	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo3	0%	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60%	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90%	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1 (见注 2)	0%	2.5E-06			5.0E-06			>1.0E-05		
	60%	1.0E-06			2.0E-06			1.0E-05		
	90%	2.5E-07			5.0E-07			2.5E-06		
	99%	2.5E-08			5.0E-08			2.5E-07		

表 B.10（续）

结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo2	0%	5.4E-08	2.5E-07	5.0E-07	1.2E-07	5.2E-07	1.0E-06	9.5E-07	2.9E-06	5.3E-06
	60%	3.7E-08	1.8E-07	3.5E-07	7.7E-08	3.6E-07	7.1E-07	5.4E-07	1.9E-06	3.6E-06
	90%	2.8E-08	1.4E-07	2.8E-07	5.7E-08	2.8E-07	5.5E-07	3.3E-07	1.4E-06	2.8E-06
	99%	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.7E-07	1.3E-06	2.5E-06
2oo2（见注 2）	0%	5.0E-06			1.0E-05			>1.0E-05		
	60%	2.0E-06			4.0E-06			>1.0E-05		
	90%	5.0E-07			1.0E-06			5.0E-06		
	99%	5.0E-08			1.0E-07			5.0E-07		
1oo2D	0%	5.4E-08	2.5E-07	5.0E-07	1.2E-07	5.2E-07	1.0E-06	9.5E-07	2.9E-06	5.3E-06
	60%	3.6E-08	1.8E-07	3.5E-07	7.3E-08	3.5E-07	7.0E-07	4.3E-07	1.8E-06	3.6E-06
	90%	2.8E-08	1.4E-07	2.8E-07	5.5E-08	2.8E-07	5.5E-07	2.8E-07	1.4E-06	2.8E-06
	99%	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-06
2oo3	0%	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.5E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60%	4.1E-08	1.8E-07	3.5E-07	9.2E-08	3.7E-08	7.2E-07	9.1E-07	2.2E-06	3.9E-06
	90%	2.9E-08	1.4E-07	2.8E-07	6.2E-08	2.8E-07	5.6E-07	4.4E-07	1.5E-06	2.9E-06
	99%	2.6E-08	1.3E-07	2.5E-07	5.2E-08	2.5E-07	5.1E-07	3.0E-07	1.3E-06	2.6E-06

注 1：此表给出了 PFH_G 的示例值，它是根据 B.1 中所列出的假设，使用 B.3.2 中的公式计算出的，如果传感器、逻辑元件、最终元件子系统仅由一个表决通道组构成，那么 PFH_G 分别与 PFH_S、PFH_L 或 PFH_{FE} 的数值相等（见 B.3.1 和 B.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均失效概率。

表 B.11　检测测试时间间隔为 3 个月，平均恢复时间为 8 h 时每小时的平均失效概率（高要求或连续操作模式下）

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1（见注 2）	0%	5.0E-08			2.5E-07			5.0E-07		
	60%	2.0E-08			1.0E-07			2.0E-07		
	90%	5.0E-09			2.5E-08			5.0E-08		
	99%	5.0E-10			2.5E-09			5.0E-09		
1oo2	0%	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60%	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90%	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

表 B.11（续）

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
2oo2（见注 2）	0%	1.0E-07			5.0E-07			1.0E-06		
	60%	4.0E-08			2.0E-07			4.0E-07		
	90%	1.0E-08			5.0E-08			1.0E-07		
	99%	1.0E-09			5.0E-09			1.0E-08		
1oo2D	0%	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60%	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.1E-09	3.5E-08	7.0E-08
	90%	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo3	0%	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08	1.2E-08	5.1E-08	1.0E-07
	60%	7.1E-10	3.5E-09	7.0E-09	3.7E-09	1.8E-08	3.5E-08	7.7E-09	3.6E-08	7.0E-08
	90%	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.7E-09	2.8E-08	5.5E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1（见注 2）	0%	2.5E-06			5.0E-06			>1.0E-05		
	60%	1.0E-06			2.0E-06			1.0E-05		
	90%	2.5E-07			5.0E-07			2.5E-06		
	99%	2.5E-08			5.0E-08			2.5E-07		
1oo2	0%	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.4E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60%	3.7E-08	1.8E-07	3.5E-07	7.9E-08	3.6E-07	7.1E-07	8.9E-07	2.2E-06	3.9E-06
	90%	2.8E-08	1.4E-07	2.8E-07	6.1E-08	2.8E-07	5.5E-07	4.2E-07	1.5E-06	2.9E-06
	99%	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.8E-07	1.3E-06	2.5E-06
2oo2（见注 2）	0%	5.0E-06			1.0E-05			>1.0E-05		
	60%	2.0E-06			4.0E-06			>1.0E-05		
	90%	5.0E-07			1.0E-06			5.0E-06		
	99%	5.0E-08			1.0E-07			5.0E-07		
1oo2D	0%	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.4E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60%	3.7E-08	1.8E-07	3.5E-07	7.9E-08	3.6E-07	7.1E-07	5.7E-06	1.9E-06	3.7E-06
	90%	2.8E-08	1.4E-07	2.8E-07	5.6E-08	2.8E-07	5.5E-07	2.9E-07	1.4E-06	2.8E-06
	99%	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-06

表 B.11（续）

结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
2oo3	0%	9.0E-08	2.8E-07	5.3E-07	2.6E-07	6.3E-07	1.1E-06	4.5E-06	5.9E-06	7.6E-06
	60%	5.1E-08	1.9E-07	3.6E-07	1.4E-07	4.1E-07	7.5E-07	2.0E-06	3.2E-06	4.7E-06
	90%	3.2E-08	1.4E-07	2.8E-07	7.2E-08	2.9E-07	5.6E-07	7.1E-07	1.8E-06	3.1E-06
	99%	2.6E-08	1.3E-07	2.5E-07	5.3E-08	2.6E-07	5.1E-07	3.2E-07	1.3E-06	2.6E-06

注 1：此表给出了 PFH_G 的示例值，它是根据 B.1 中所列出的假设，使用 B.3.2 中的公式计算出的，如果传感器、逻辑元件、最终元件子系统仅由一个表决通道组构成，那么 PFH_G 分别与 PFH_S、PFH_L 或 PFH_{FE} 的数值相等（见 B.3.1 和 B.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均失效概率。

表 B.12　检验测试时间间隔为 6 个月，平均恢复时间为 8 h 时每小时的平均失效概率（高要求或连续操作模式下）

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1（见注 2）	0%	5.0E-08			2.5E-07			5.0E-07		
	60%	2.0E-08			1.0E-07			2.0E-07		
	90%	5.0E-09			2.5E-08			5.0E-08		
	99%	5.0E-10			2.5E-09			5.0E-09		
1oo2	0%	1.0E-09	5.0E-09	1.0E-08	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07
	60%	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.4E-09	3.5E-08	7.0E-08
	90%	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo2（见注 2）	0%	1.0E-07			5.0E-07			1.0E-06		
	60%	4.0E-08			2.0E-07			4.0E-07		
	90%	1.0E-08			5.0E-08			1.0E-07		
	99%	1.0E-09			5.0E-09			1.0E-08		
1oo2D	0%	1.0E-09	5.0E-09	1.0E-08	5.5E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07
	60%	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90%	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo3	0%	1.0E-09	5.0E-09	1.0E-08	5.8E-09	2.6E-08	5.1E-08	1.3E-08	5.3E-08	1.0E-07
	60%	7.1E-10	3.5E-09	7.0E-09	3.8E-09	1.8E-08	3.5E-08	8.3E-09	3.6E-08	7.1E-08
	90%	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.8E-09	2.8E-08	5.5E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

表 B.12（续）

结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1（见注 2）	0%	2.5E-06			5.0E-06			>1.0E-05		
	60%	1.0E-06			2.0E-06			1.0E-05		
	90%	2.5E-07			5.0E-07			2.5E-06		
	99%	2.5E-08			5.0E-08			2.5E-07		
1oo2	0%	7.6E-08	2.7E-07	5.2E-07	2.1E-07	5.9E-07	1.1E-06	3.1E-06	4.7E-06	6.8E-06
	60%	4.6E-08	1.8E-07	3.6E-07	1.1E-07	3.9E-07	7.3E-07	1.4E-06	2.7E-06	4.3E-06
	90%	3.0E-08	1.4E-07	2.8E-07	6.6E-08	2.9E-07	5.6E-07	5.5E-07	1.6E-06	3.0E-06
	99%	2.6E-08	1.3E-07	2.5E-07	5.2E-08	2.5E-07	5.1E-07	2.9E-07	1.3E-06	2.6E-06
2oo2（见注 2）	0%	5.0E-06			1.0E-05			>1.0E-05		
	60%	2.0E-06			4.0E-06			>1.0E-05		
	90%	5.0E-07			1.0E-06			5.0E-06		
	99%	5.0E-08			1.0E-07			5.0E-07		
1oo2D	0%	7.6E-08	2.7E-07	5.2E-07	2.1E-07	5.9E-07	1.1E-06	3.1E-06	4.7E-06	6.8E-06
	60%	3.9E-08	1.8E-07	3.6E-07	8.7E-07	3.7E-07	7.1E-07	7.8E-06	2.1E-06	3.8E-06
	90%	2.8E-08	1.4E-07	2.8E-07	5.6E-08	2.8E-07	5.5E-07	3.0E-07	1.4E-06	2.8E-06
	99%	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-06
2oo3	0%	1.3E-07	3.2E-07	5.5E-07	4.2E-07	7.7E-07	1.2E-06	8.4E-06	9.2E-06	1.0E-06
	60%	6.7E-08	2.0E-07	3.7E-07	2.0E-07	4.6E-07	8.0E-07	3.6E-06	4.6E-06	6.0E-05
	90%	3.6E-08	1.5E-07	2.8E-07	8.8E-08	3.1E-07	5.8E-07	1.1E-06	2.1E-06	3.4E-06
	99%	2.6E-08	1.3E-07	2.5E-07	5.5E-08	2.6E-07	5.1E-07	3.6E-07	1.4E-06	2.6E-06

注 1：此表给出了 PFH_G 的示例值，它是根据 B.1 中所列出的假设，使用 B.3.2 中的公式计算出的，如果传感器、逻辑元件、最终元件子系统仅由一个表决通道组构成，那么 PFH_G 分别与 PFH_S、PFH_L 或 PFH_{FE} 的数值相等（见 B.3.1 和 B.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均失效概率。

表 B.13 检验测试时间间隔为 1 年以及平均恢复时间为 8 h 时每小时的平均失效概率（高要求或连续操作模式下）

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1（见注 2）	0%	5.0E-08			2.5E-07			5.0E-07		
	60%	2.0E-08			1.0E-07			2.0E-07		
	90%	5.0E-09			2.5E-08			5.0E-08		
	99%	2.0E-10			2.5E-09			5.0E-09		

表 B.13（续）

结构	DC	λ=1.0E-07			λ=5.0E-07			λ=1.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo2	0%	1.0E-09	5.0E-09	1.0E-08	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07
	60%	7.1E-10	3.5E-09	7.0E-09	3.7E-09	1.8E-08	3.5E-08	7.9E-09	3.6E-08	7.1E-08
	90%	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.7E-09	2.8E-08	5.5E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo2（见注 2）	0%	1.0E-07			5.0E-07			1.0E-06		
	60%	4.0E-08			2.0E-07			4.0E-07		
	90%	1.0E-08			5.0E-08			1.0E-07		
	99%	1.0E-09			5.0E-09			1.0E-08		
1oo2D	0%	1.0E-09	5.0E-09	1.0E-08	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07
	60%	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.3E-09	3.5E-08	7.1E-08
	90%	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo3	0%	1.1E-09	5.1E-09	1.0E-08	6.6E-09	2.6E-08	5.1E-08	1.6E-08	5.5E-08	1.0E-07
	60%	7.3E-10	3.5E-09	7.0E-09	4.1E-09	1.8E-08	3.5E-08	9.6E-09	3.7E-08	7.2E-08
	90%	5.6E-10	2.8E-09	5.5E-09	2.9E-09	1.4E-08	2.8E-08	6.2E-09	2.8E-08	5.6E-08
	99%	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo1（见注 2）	0%	2.5E-06			5.0E-06			>1.0E-05		
	60%	1.0E-06			2.0E-06			1.0E-06		
	90%	2.5E-07			5.0E-07			2.5E-06		
	99%	2.5E-08			5.0E-08			2.5E-07		
1oo2	0%	1.0E-07	2.9E-07	5.4E-07	3.1E-07	6.8E-07	1.1E-06	5.8E-06	6.9E-06	8.5E-06
	60%	5.6E-08	1.9E-07	3.7E-07	1.6E-07	4.3E-07	7.7E-07	2.5E-06	3.7E-06	5.1E-06
	90%	3.3E-08	1.4E-07	2.8E-07	7.7E-08	2.9E-07	5.7E-07	8.2E-07	1.9E-06	3.2E-06
	99%	2.6E-08	1.3E-07	2.5E-07	5.3E-08	2.5E-07	5.1E-07	3.2E-07	1.3E-06	2.6E-06
2oo2（见注 2）	0%	5.0E-06			1.0E-06			>1.0E-05		
	60%	2.0E-06			4.0E-06			>1.0E-05		
	90%	5.0E-07			1.0E-06			5.0E-06		
	99%	5.0E-08			1.0E-07			5.0E-07		

表 B.13（续）

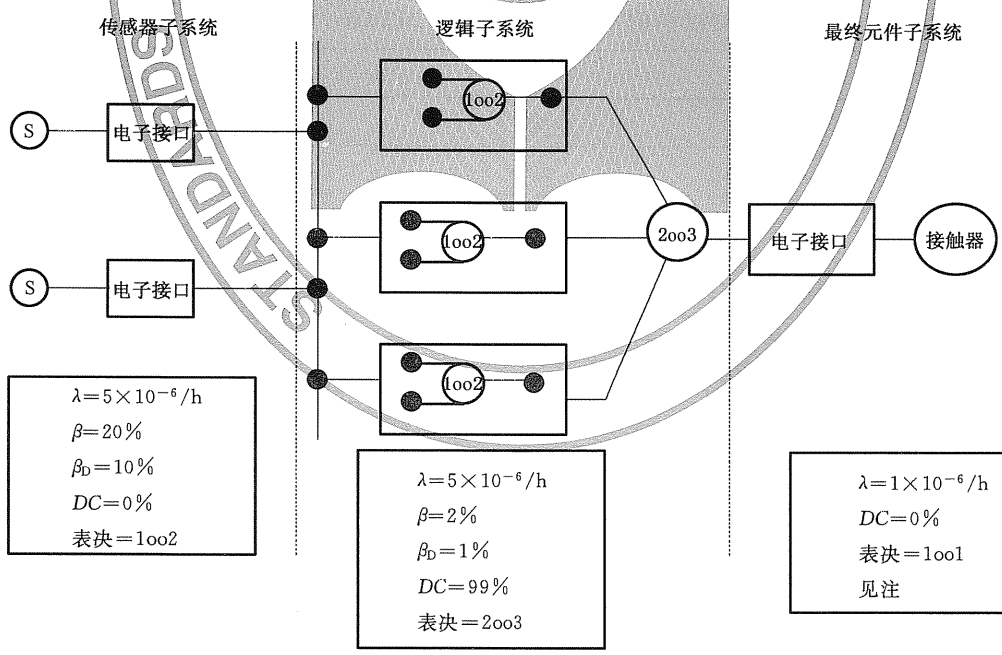
结构	DC	λ=5.0E-06			λ=1.0E-05			λ=5.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%	β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo2D	0%	1.0E-07	2.9E-07	5.4E-07	3.1E-07	6.8E-07	1.1E-06	5.8E-06	6.9E-06	8.5E-06
	60%	4.4E-08	1.8E-07	3.6E-07	1.0E-07	3.8E-07	7.3E-07	1.2E-06	2.5E-06	4.1E-06
	90%	2.8E-08	1.4E-07	2.8E-07	5.7E-08	2.8E-07	5.5E-07	3.3E-07	1.4E-06	2.8E-06
	99%	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-06
2oo3	0%	2.1E-07	3.8E-07	6.1E-07	7.3E-07	1.0E-06	1.4E-06	>1.0E-05	>1.0E-05	>1.0E-05
	60%	9.9E-08	2.3E-07	4.0E-07	3.3E-07	5.8E-07	9.0E-07	6.8E-06	7.5E-06	8.4E-06
	90%	4.4E-08	1.5E-07	2.9E-07	1.2E-07	3.3E-07	6.0E-07	1.9E-06	2.9E-06	4.1E-06
	99%	2.7E-08	1.3E-07	2.5E-07	5.8E-08	2.6E-07	5.1E-07	4.4E-07	1.4E-06	2.7E-06

注 1：此表给出了 PFH_G 的示例值，它是根据 B.1 中所列出的假设，使用 B.3.2 中的公式计算出的，如果传感器、逻辑元件、最终元件子系统仅由一个表决通道组构成，那么 PFH_G 分别与 PFH_S、PFH_L 或 PFH_{FE} 的数值相等（见 B.3.1 和 B.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均失效概率。

B.3.4 高要求或连续操作模式的示例

考虑需要一个 SIL2 系统的安全功能。假设按前面的作法对系统结构的初始评估是，针对 1 组 2 个传感器结构为表决 1oo2。逻辑子系统是配置为冗余 2oo3D 的 PES，用于驱动 1 个停机接触器。如图 B.14 所示，初始评估时假设检验测试周期为 6 个月。



注：最终元件子系统的总安全失效分数大于 60%。

图 B.14 高要求或连续操作模式的结构示例

表 B.14 高要求或连续操作模式结构示例中传感器子系统每小时的失效概率
（检验测试的时间间隔为 6 个月，*MTTR* 为 8 h）

结构	*DC*	λ=5.0E-06		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
1oo2	0%	7.6E-08	2.7E-07	5.2E-07
	60%	4.6E-08	1.8E-07	3.6E-07
	90%	3.0E-08	1.4E-07	2.8E-07
	99%	2.6E-08	1.3E-07	2.5E-07
注：此表摘自表 B.12。				

表 B.15 高要求或连续操作模式结构示例中逻辑子系统每小时的失效概率
（检验测试的时间间隔为 6 个月，*MTTR* 为 8 h）

结构	*DC*	λ=1.0E-05		
		β=2% β_D=1%	β=10% β_D=5%	β=20% β_D=10%
2oo3	0%	4.2E-07	7.7E-07	1.2E-06
	60%	2.0E-07	4.6E-07	8.0E-07
	90%	8.8E-08	3.1E-07	5.8E-07
	99%	5.5E-08	2.6E-07	5.1E-07
注：此表摘自表 B.12。				

表 B.16 高要求或连续操作模式结构示例中最终元件子系统每小时的失效概率
（检验测试的时间间隔为 6 个月 *MTTR* 为 8 h）

结构	*DC*	λ=1.0E-06
1oo1	0%	5.0E-07
	60%	2.0E-07
	90%	5.0E-06
	99%	5.0E-09
注：此表摘自表 B.12。		

从表 B.11～表 B.16 中可获得出下列数值。

对于传感器子系统

$$PFH_S = 5.2\times10^{-7}/\text{h}$$

对于逻辑子系统

$$PFH_L = 5.5\times10^{-8}/\text{h}$$

对于最终元件子系统

$$PFH_{FE} = 5.0\times10^{-7}/\text{h}$$

因此，对于安全功能

$$PFH_{SYS} = 5.2\times10^{-7} + 5.5\times10^{-8} + 5.0\times10^{-7}$$
$$= 1.1\times10^{-6}/\text{h}$$

≡安全完整性等级 1

为了改善系统以满足安全完整性等级 2，需要进行如下步骤之一：

a) 改变输入传感器类型和安装以提高对共同原因失效的防卸能力，因此要将 β 从 20% 改进为 10%，β_D 从 10% 改进为 5%。

$PFH_S = 2.7 \times 10^{-7}/h$

$PFH_L = 5.5 \times 10^{-8}/h$

$PFH_{FE} = 5.0 \times 10^{-7}/h$

$PFH_{SYS} = 8.3 \times 10^{-7}/h$

≡ 安全完整性等级 2

b) 在 1oo2 中将单一输出设备改变为两个设备（$\beta = 10\%$，$\beta_D = 5\%$）

$PFH_S = 5.2 \times 10^{-7}/h$

$PFH_L = 5.5 \times 10^{-8}/h$

$PFH_{FE} = 5.1 \times 10^{-8}/h$

$PFH_{SYS} = 6.3 \times 10^{-7}/h$

≡安全完整性等级 2

B.4 参考

参考文献[1]～[6]给出了评价失效概率更加详细的说明。

附 录 C
（资料性附录）
诊断覆盖率和安全失效分数的计算：工作示例

计算诊断覆盖和安全失效分数的方法在 GB/T 20438.2—2006 附录 C 中已经给出。在此附录中简要地描述了如何使用该方法计算 E/E/PE 安全相关系统诊断覆盖率。假设在需要获得表 C.1 所示值时，GB/T 20438.2 中规定的所有信息均可使用。表 C.2 给出了 E/E/PE 安全相关系统部件或子系统可申明的诊断覆盖率的限制，表 C.2 中的数值是基于工程判断得出的。

为了理解表 C.1 中所有数值的意义，需要一个详细的硬件原理图，从中可以确定所有失效模式的效应。这些数值仅仅是一些例子，例如，因为实际上不可能检测所有部件的失效模式，假设表 C.1 中某些部件无诊断覆盖率。

从表 C.1 中可得到如下内容：

a) 不用诊断测试已执行了失效模式和效应分析从而确定每个部件每种失效模式对系统行为的效应。显示了每个部件与每种失效模式相关的总失效率分数，并分为安全(S)失效和危险(D)失效两部分。对于简单部件来说，安全失效和危险失效的划分可能是确定性的，其他情况则基于工程判断。对于复杂部件，不能对失效模式进行详细分析时，通常将失效分为安全失效 50%，危险失效 50%，对于此表，已经使用了 a)中给定的失效模式，虽然其他划分失效模式的方法可能会更好。

b) “DC_{comp}”列中给出了每个部件每种具体的诊断测试的诊断覆盖率，还给出了用来检测安全和危险失效专用诊断覆盖率。虽然简单部件的短路和开路失效可以被 100%的诊断覆盖率检测到。但是在使用表 C.2 时 U16(复杂的 B 型部件)的诊断覆盖率已限定为 90%。

c) (1)列和(2)列给出了不存在诊断测试时，每个部件的安全失效率和危险失效率(分别为 λ_S 和 $\lambda_{DD}+\lambda_{DU}$)。

d) 可以把检测到的一个危险失效当作实际上的安全失效。因此会发现可按实际上的安全失效(即检测到的安全失效、未检测到的安全失效或检测到的危险失效)和未检测到的危险失效来划分失效。实际上有效的安全失效率等于危险失效率乘以具体的诊断覆盖率，然后把结果与安全失效率相加(见(3)列)。同样，未检测到的危险失效率可由 1 减去危险失效的具体诊断覆盖率，然后将结果同危险失效率相乘而得出（见(4)列)。

e) (5)列给出了检测到的安全失效率，(6)列给出了检测到的危险失效率，它们分别由具体诊断覆盖率分别乘以危险失效率和安全失效率得出。

f) 表中产生了如下结果：

∴ 总安全失效率（包括检测到的危险失效） $\sum\lambda_S+\sum\lambda_{DD}=9.9\times10^{-7}$

未检测到的总危险失效率 $\sum\lambda_{DU}=5.1\times10^{-8}$

总失效率 $\sum\lambda_S+\sum\lambda_{DD}+\sum\lambda_{DU}=1.0\times10^{-6}$

未检测到的总安全失效率 $\sum\lambda_{SU}=2.7\times10^{-8}$

安全失效的诊断覆盖率 $\dfrac{\sum\lambda_{SD}}{\sum\lambda_S}=\dfrac{3.38}{3.65}=93\%$

危险失效的诊断覆盖率 $\dfrac{\sum\lambda_{DD}}{\sum\lambda_{DD}+\sum\lambda_{DU}}=\dfrac{6.21}{6.72}=92\%$（通常称为诊断覆盖率）

安全失效分数 $\dfrac{\sum\lambda_S+\sum\lambda_{DD}}{\sum\lambda_S+\sum\lambda_{DD}+\sum\lambda_{DU}}=\dfrac{986}{365+672}=95\%$

g) 无诊断测试时失效率的分为：安全失效 35%，危险失效 65%。

表 C.1 计算诊断覆盖率和安全失效分数示例

项	数量	类型	每种失效模式安全失效与危险失效的分割								诊断覆盖率中安全失效与危险失效的分割以及计算的失效率($\times10^{-9}$)						
			OC		SC		Drift		Function		DC_{comp}		(1)	(2)	(3)	(4)	(5)	(6)
			S	D	S	D	S	D	S	D	S	D	λ_S	$\lambda_{DD}+\lambda_{DU}$	$\lambda_S+\lambda_{DD}$	λ_{DU}	λ_{SD}	λ_{DD}
Print	1	Print	0.5	0.5	0.5	0.5	0	0	0	0	0.99	0.99	11.0	11.0	21.9	0.1	10.9	10.9
CN1	1	Con96pin	0.5	0.5	0.5	0.5					0.99	0.99	11.5	11.5	22.9	0.1	11.4	11.4
C1	1	100nF	1	0	1	0	0	0	0	0	1	0	3.2	0.0	3.2	0.0	3.2	0.0
C2	1	10μF	0	0	1	0	0	0	0	0	1	0	0.8	0.0	0.8	0.0	0.8	0.0
R4	1	1M	0.5	0.5	0.5	0.5					1	1	1.7	1.7	3.3	0.0	1.7	1.7
R6	1	100K									0	0	0.0	0.0	0.0	0.0	0.0	0.0
OSC1	1	OSC24MHz	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	1	1	16.0	16.0	32.0	0.0	16.0	16.0
U8	1	74HCT85	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.99	0.99	22.8	22.8	45.4	0.2	22.6	22.6
U16	1	MC6800012	0	1	0	1	0.5	0.5	0.5	0.5	0.90	0.90	260.4	483.6	695.6	48.4	234.4	435.2
U26	1	74HCT74	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.99	0.99	22.8	22.8	45.4	0.2	22.6	22.6
U27	1	74F74	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.99	0.99	14.4	14.4	28.7	0.1	14.3	14.3
U28	1	PAL16L8A	0	1	0	1	0	1	0	1	0.98	0.98	0.0	88.0	86.2	1.8	0.0	86.2
T1	1	BC817	0	0	0	0.67	0	0.5	0	0	1	1	0.0	0.2	0.4	0.0	0.0	0.2
总计													365	672	986	50.9	338	621

注：R6 项中未检测出任何失效模式，但失效不会影响安全或可用性。

关键词：

S	安全失效
D	危险失效
OC	开路
SC	短路
Drift	值的改变
Function	功能失效
DC_{comp}	部件的具体诊断覆盖率

另见表 B.1，在此表中失效率是针对讨论中的那些部件，而不是针对通道中的每个部件的。

表 C.2 不同子系统的诊断覆盖率和有效性

部　　件	低诊断覆盖率	中诊断覆盖率	高诊断覆盖率
CPU(见注 3)	全部小于 70%	全部小于 90%	99%～99.99%
寄存器，内部 RAM	50%～70%	85%～90%	—
编码和执行，包括标志寄存器	50%～60%	75%～95%	—
(见注 3)	50%～70%	85%～98%	85%～98%
地址计算(见注 3)	50%～60%	60%～90%	
程序计数器，堆栈指针	50%～70%		
	40%～60%		
BUS(总线)			
内存管理单元	50%	70%	90%～99%
总线仲裁	50%	70%	90%～99%
中断处理	40%～60%	60%～90%	85%～98%
时钟(石英)(见注 4)	50%	—	95%～99%
程序流监视			
时序的(见注 3)	40%～60%	60%～90%	—
逻辑的(见注 3)	40%～60%	60%～90%	—
时序和逻辑的(见注 5)		60%～90%	90%～98%
不可变的内存	50%～70%	99%	99.99%
可变的内存	50%～70%	85%～90%	99%～99.99%
分离的硬件			
数字 I/O	70%	90%	99%
模拟 I/O	50%～60%	70%～85%	99%
电源	50%～60%	70%～85%	99%
通信和大容量存储器	90%	99.9%	99.99%
机电装置	90%	99%	99.9%
传感器	50%～70%	70%～85%	99%
最终元件	50%～70%	70%～85%	99%

注 1：此表应与 GB/T 20438.2—2006 中表 A.1 一起来阅读，表 A.1 提供了考虑到的各种失效模式。

注 2：在给定诊断覆盖率范围的情况下，只对要求严格的监视方式，或使用高度动态方式测试重要功能的测试措施，才有可能需要设置时间间隔上限。

注 3：对于没有高诊断覆盖率数值的技术，目前还没有高效的措施和技术。

注 4：目前，还没有针对石英钟的中等有效的措施和技术。

注 5：用于监视时序程序流和逻辑程序流组合的最小诊断覆盖率为中等。

参考文献为[7]～[9]。

附 录 D
（资料性附录）
量化 E/E/PE 系统中硬件共同原因失效效应的方法

D.1 概述

GB/T 20438 包括了许多处理系统失效的措施。但是无论这些措施被应用得多好，还是存在系统残余失效发生的概率。虽然这不会严重影响到单通道系统的可靠性计算，但是可能对多通道系统中多个通道失效（即共同原因失效）具有潜在影响，使得可靠性计算应用于多通道系统中时会导致严重的错误。

本附录描述了一种方法，准许在多通道 E/E/PE 系统的安全评估中考虑共同原因失效。相对于忽略潜在的共同原因失效而言，此方法的使用给出了对系统完整性更加精确的估算。

使用此方法计算 β 值，β 系数常用于共同原因失效的建模中。在两个或更多个系统并行操作应用中，它可以用来根据那些系统之一的随机硬件失效估算共同原因失效率（见 D.5）。一些可替代的方法在某些情况下可能更加适合，例如，从共同原因失效的可用数据中，能够获得一个被证明更加精确的 β 系数。

D.2 简述

系统失效被认为是由两种原因产生的：

——随机硬件失效；和

——系统失效。

假设前者对任何部件而言在时间上是随机发生的，并且导致系统中构成系统一部分的部件即通道的失效。在多通道系统中所有通道发生独立硬件随机失效，从而使所有通道同时处于故障状态的概率是有限的。因为，随机硬件失效被假设在时间上是随机发生的，与单通道失效概率相比，同时发生影响其他并行通道的这种失效的概率是很低的。可以使用建立好的技术计算此概率。

然而，有些失效，即由单一原因引起的共同原因失效，可影响多个通道。它们可能是一个系统故障引起的（例如：设计或规范失误），或者由一个外部应力导致一个早期的随机硬件失效引起的（例如公用冷却风扇的随机硬件失效引起的温度过高，导致部件寿命缩短或使它们不能在规定的环境下工作），或者是上述两种情况共同导致的。由于在多通道系统中，共同原因失效可能会影响多个通道，共同原因的失效的概率就可能成为多通道系统中决定总的失效概率的主要因素，并且如果不考虑这一点就不能真实地估算组合系统的安全完整性等级。

虽然共同原因失效是由单一原因导致的，但是它们不会在所有通道中同时出现。例如如果冷却风扇出了故障，多通道 E/E/PE 系统的所有通道都会出故障，从而导致共同原因失效。但所有通道变热的速度不同，或有相同的临界温度，因此不同通道发生失效的时间各不相同。

可编程系统的结构准许系统在线运行时执行内部诊断测试功能，可使用的实现方法很多，例如：

——能够连续检查单通道 PES 系统内部工作并同时检查输入及输出设备的功能。如果从开头就进行有计划的设计，测试覆盖率可以达到 99%[10]。如果在导致失效之前 99%的内部故障都被揭露出来了，结果单一通道故障对共同原因失效的贡献将大大减少。

——除内部测试之外，PES 系统中每一个通道均可监视多通道 PES 系统中的其他通道（或者在一个多 PE 系统中每一个 PE 设备均可监测另一个 PE 设备）的输出。因此，如果在一个通道中发生失效，可以通过其他一个或多个没有发生故障的通道或执行交叉监测的通道发现失效并安全地关机（值得注意的是，交叉监测只有在控制系统不断改变状态下才会有效，例如常用于

循环机械中保护装置的互锁功能，或者引入短暂改变不会影响受控功能时）。交叉监测可在较高频率下进行，因此，刚好可以在发生非同步共同原因失效之前，交叉监视就能检测到因第一个通道的故障而导致的失效，并可在第二通道受到影响之前，使系统进入某种安全状态。

在冷却风扇的事例中，温度升高速率以及每个通道敏感性的差别非常小，因此在第一个通道发生故障几十分钟之后，可能第二个通道才发生故障。从而允许诊断测试在第二个通道发生共同原因失效之前启动安全关机。

上述结论如下：

——基于 PE 的系统具有防御共同原因失效的潜力，因此同其他技术相比对共同原因失效的敏感性更低。

——与其他技术相比，不同的 β 系数都能适用于基于 PE 的系统。因此基于历史数据估算的 β 系数可能不适用（不存在用于估算共同原因失效概率的研究模型以供研究自动交叉监视的效应之用）。

——因为按时间分布的共同原因失效，在它们可能影响到所有通道之前就被诊断测试揭露出来了，因此这样的失效不会看作为共同原因失效并被报告。

有三种方法可以用来减少潜在的危险共同原因失效的概率：

a) 减少随机硬件和系统失效的总数（减少部分为图 D.1 中两椭圆相重合的部分）。

b) 使通道最大程度的独立（减少图 D.1 中两椭圆间重合部分的总量，同时维持它们的原来的面积）。

c) 仅有一个通道受到影响，在下一个通道被影响之前诊断测试就已把共同原因失效揭露出来了。

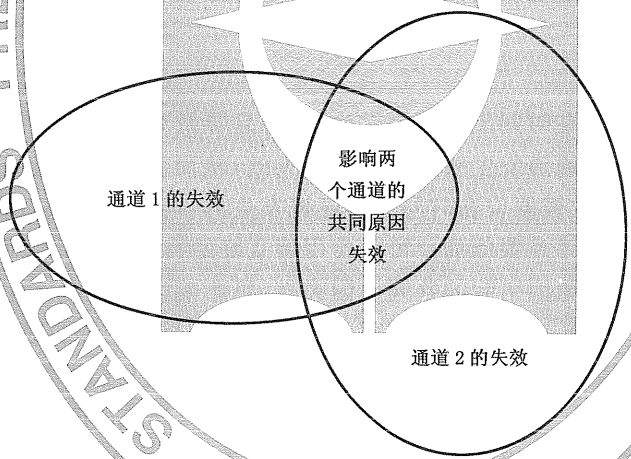


图 D.1 各个通道失效与共同原因失效的关系

此方法以上述三条为基础，并需要 个三方面的方法。

a) 使用 GB/T 20438 中规定的技术，将整个系统失效的概率减少到与随机硬件失效的概率同数量级的水平。

b) 量化那些能够被量化的系数，即如：GB/T 20438.2 规定的那样考虑随机硬件的失效概率。

c) 通过考虑目前最实际的途径得出与随机硬件失效概率有关的共同原因失效概率的系数。获得该系数的方法在本附录中已作了描述。

大多数估算共同原因失效概率的方法均试图从随机硬件失效概率中进行预测。显然，对这些概率之间的任何直接关系的正确性证明十分贫乏，然而，在实践中已经发现这样的相互关系，并且很可能是二次效应的结果。例如系统随机硬件失效概率越高：

a) 系统需要的维护量就越高，在维护时引入的系统故障的概率取决于执行维护的次数，而且这也会对导致共同原因失效的人为错误率产生影响。这将会导致随机硬件失效概率与共同原因失

效概率之间的关系。例如：

——当每次随机硬件失效发生时，紧随测试之后就需要进行修理，可能还要重新校准。

——对于给定的安全完整性等级，随机硬件失效概率越高的系统需要执行的检验测试就越频繁，其深度和复杂程度也越大，这又增加了人为干扰。

b) 系统也越复杂，发生随机硬件失效的概率依赖于系统部件的数量，因此也依赖于系统的复杂性。复杂的系统不容易被了解，就更易导致系统故障。此外，无论是通过分析或测试，系统的复杂性都会使其更难检测到故障，并会导致系统逻辑部分不能运用（极少的情况除外），还会导致随机硬件失效概率与共同原因失效率概率之间的关联。

尽管，目前的模型存在着种种限制，但是要相信它们代表了目前最先进的评价多通道系统中共同原因失效的方法。本附录中阐述的方法采用了与建立完善的 β 系数模型相同的方法，如已经描述过的三方面方法中的第三部分。

下面是在 E/E/PE 系统上使用 β 系数模型时所遇到的两个难点：

——应该选择什么样的 β 系数值？很多原始资料（例如参考文献[10]）建议 β 系数值可能出现的范围，但是没有给出确切的值，使得用户只能做出主观选择。为了克服这个问题，本附录中所述的方法是基于参考文献[11]中有关系统的原始描述，最近已在参考文献[12]中重新定义。

——β 系数模型没有考虑到现代 PES 经改进的诊断测试能力，它可以用来在非同步共同原因失效有足够时间充分显现之前就检测到它。为了克服这个不足，已经修改了参考文献[11]和[12]中描述的方法，以便反映诊断测试对可能的 β 值估算的影响。

在 PES 中运行的诊断测试功能不断地将 PES 的工作与预定义的状态相比较，这些状态能以软件和硬件形式预先定义（如看门狗）。据此，诊断测试功能可以被看作是一个附加的、部分不同的、与 PES 并行的通道。

在通道之间还可以执行交叉监视。此项技术已在只基于继电器的双通道互锁系统中使用多年了。但是使用继电器技术，通常只有当通道转变状态时，才可以用来执行交叉检查，当系统长时间保持同一状态时，这种测试不适合用来揭露非同步共同原因失效。因为在这种情况下系统长期保持在同一状态下（例如 ON）使用 PES 技术，交叉监视能以高重复频率执行。

D.3 方法的范围

方法的范围局限于硬件的共同原因失效，其原因如下：

——β 系数模型把随机硬件失效的概率同共同原因失效的概率联系起来了。包括整个系统的共同原因失效概率取决于系统的复杂性（可能由用户软件决定），并不仅仅取决于硬件。很显然，基于随机硬件失效概率的任何计算方式都不考虑软件的复杂性。

——有关共同原因失效的报告通常限于硬件失效，即硬件制造商最关心的领域。

——实际上，并不认为建立系统失效模型是可行的（例如软件失效）。

——GB/T 20438.3 中规定的措施是为了将软件的共同原因失效的概率降低到可以接受的目标安全完整性等级。

因此，根据此方法得出的共同原因失效概率的估算仅与硬件失效有关。并且，不应假定利用此方法能够获得包括相关软件失效概率在内的总失效概率。

D.4 方法中考虑的要点

由于传感器、逻辑子系统以及最终元件容易受到诸如不同环境条件和不同能力水平的诊断测试的影响，因此，此方法应在每种子系统中分别使用。例如，逻辑子系统更多的是在受控环境中使用，而传感器可安装在工程管道外部，暴露在自然环境中。

可编程电子通道有执行经改进的诊断测试功能的潜力，它们能够：

——在通道中拥有较高的诊断覆盖率；

——监测附加的冗余通道；

——具有高重复率；并且

——在增加用例数的情况下，仍旧可以监测传感器和/或最终元件。

在受到影响的所有通道中，大部分共同原因失效并不同时发生，因此，如果诊断测试的重复频率足够高时，可以揭露出大部分共同原因失效，从而在它们影响所有的可用通道之前得以避免。

诊断测试并不能评价一个多通道系统的所有特性，这些特性都对共同原因失效的免疫力有影响。然而，与多样性或独立性相关的这些特性会更有效。非同步共同原因失效中，任何可以提高通道失效间隔时间（或者减少同步共同原因失效分数）的特性，均可提高诊断测试检测到失效并使设备处于安全状态的概率。所以有关共同原因失效免疫力的特性可分成两部分，即可认为通过使用诊断测试能增加其效果的那部分特性和不能提高其效果的那部分特性。这就产生了两列，在表 D.1 中分别用 X、Y 表示。

虽然，对于三通道系统，影响所有三个通道的共同原因失效的概率可能小于影响两个通道的失效概率，但为了简化方法，假设概率是与受到影响的通道数无关的，也就是说，假设当发生一次共同原因失效时，它将影响所有通道。

不存在用于校准方法的有关硬件共同原因失效已知数据的方法，所以，此附录中的表均以工程判断为基础。

有时候，并不将诊断测试例行程序看作具有直接的安全作用，所以它可不接收与提供主要控制功能的例行程序相同的质量等级。此方法是在假设诊断测试的完整性与目标安全完整性等级大小相当的基础上开发出来的。因此，开发任何基于诊断测试例行程序的软件均需使用与目标安全完整性等级相适合的技术。

D.5 使用 β 系数计算 E/E/PE 安全相关系统中共同原因失效的失效概率

考虑在多通道系统中的每一个通道中执行诊断测试时，共同原因失效对该系统的效应。

在应用 β 系数模型时，危险的共同原因失效的概率为 $\lambda_D\beta$。

其中 λ_D 为各个通道随机硬件危险失效的概率，β 为无诊断测试时的 β 系数，也就是影响所有通道的单一通道的失效分数。

假设共同原因失效影响所有通道，而且与连续共同原因失效的时间间隔相比，第一个通道被影响和所有通道被影响之间的时间间隔要小。

假设每一个通道中均执行诊断测试来检测和揭露一部分失效，并且将所有失效分为两大类：在诊断测试覆盖范围之外的一类（因此绝不可能被检测到的）以及在诊断测试覆盖范围之内的一类（因此总可以通过诊断测试检测到的）。

危险共同原因失效引起的总失效概率为：

$$\lambda_{DU}\beta+\lambda_{DD}\beta_D$$

式中：

λ_{DU}——单一通道中未检测到的失效概率，即诊断测试覆盖范围之外的失效概率，很显然，诊断测试重复率造成的任何 β 系数的任何减少均不会对这部分失效产生影响。

β——不可能检测到的危险故障的共同原因失效系数，它等于在没有诊断测试时应用的总 β 系数。

λ_{DD}——检测到单一通道的失效概率，即在诊断测试范围内单一通道的失效概率；此时，如果诊断测试的重复率高，则有一部分失效将被揭露出来，从而导致 β，即 β_D 值减小。

β_D——可检测到危险故障的共同原因失效系数。当诊断测试的重复率提高时，β_D 的值越来越小，并下降到 β 之下。

β 可从表 D.4 中获得，计算公式为 $S=X+Y$（见 D.6）。

β_D 可从表 D.4 中获得，计算公式为 $S_D=X(Z+1)+Y$。

D.6 使用表来估算 β

传感器、逻辑子系统、最终元件的 β 系数应分别计算。

为了最大限度地减小发生共同原因失效的概率，首先要建立有效的防御故障发生的措施。在系统中使用适当的措施，可以减少在估算共同原因失效引起的系统失效时使用的 β 系数的值。

表 D.1 列出了各种措施并包含了基于工程判断的相关值，这些值代表了每种措施在减少共同原因失效中所起的作用。由于对传感器与最终元件的处理与对可编程电子的处理有所不同。因此，表中用于可编程电子和传感器或最终元件的计算各列一列。

在可编程电子系统中能够结合进扩展的诊断测试，从而允许检测非同步发生的共同原因失效。为了允许在 β 系数估算中考虑诊断测试，根据工程判断将表 D.1 中每种措施的总贡献分为 X、Y 两类，每种措施的 $X:Y$ 比值，表示了诊断测试能提高该措施抗共同原因失效的作用的程度。

表 D.1 的用户应确定该系统应使用哪些措施，并把每个逻辑子系统列 X_{LS}、Y_{LS}，传感器或最终元件列 X_{SF}、Y_{SF} 中所示的相应值加起来，它们的总和分别表示为 X、Y 列。

根据诊断测试的频率和覆盖率，并考虑到重要的注 4(它限制了何时才可使用非零 Z 值)。S 值可以通过相应的下列公式进行计算。(见前章)

——$S=X+Y$ 可以得到 β 的值(未检测到的故障的 β 系数)；

——$S_D=X(Z+1)+Y$ 可以得到 β_D 的值(检测到的故障的 β 系数)。

这里，S 与 S_D 为表 D.4 中用来确定相应的 β 系数值的得分。

表 D.1 可编程电子或传感器或最终元件的评分

项　　目	逻辑子系统		传感器和最终元件	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
分离/隔开				
在所有位置，各通道的全部信号电缆布线是否都已分隔开？	1.5	1.5	1.0	2.0
逻辑子系统的所有通道的印制电路板是否是单独的？	3.0	1.0		
逻辑子系统通道是否在各自的框架中？	2.5	0.5		
如果传感器/最终元件拥有专用的控制电子电路，那么每个通道的电子电路是否分别位于各自的印制电路板上？			2.5	1.5
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
如果传感器/最终元件拥有确定的控制电子电路，那么每一个通道的电子电路是否分别位于室内各自的控制台内？			2.5	0.5
多样性与冗余				
各通道是否使用不同的电子技术？例如使用一个电子电路、可编程电子及其他继电器。	7.0			
各通道是否使用不同的电子技术？例如使用一个电子电路或其他可编程电子。	5.0			
各传感器件是否使用不同的物理原理？例如压力、温度叶片式风速计及多谱勒变换器等。			7.5	
设备均是否使用不同的电原理/设计方案？例如数字或模拟、不同的制造商(不重复标记的)或不同的技术。			5.5	

表 D.1（续）

项　　目	逻辑子系统		传感器和最终元件	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
通道是否使用具有增强冗余的 MooN 结构？其中 N>M+2。	2.0	0.5	2.0	0.5
是否使用低多样性方法？例如使用同样的技术进行硬件诊断测试。	2.0	1.0		
是否使用中等多样性方法？例如使用不同的技术进行硬件诊断测试。	3.0	1.5		
在设计活动中，各设计者设计通道时，相互之间是否不进行交流？	1.0	1.0		
在试运行期间，每个通道是否使用不同人员和不同的测试方法？	1.0	0.5	1.0	1.0
在不同时间，由不同人员对每个通道是否进行维护？	2.5		2.5	
复杂性/设计/应用/老化/经验				
通道之间的交叉连接是否能排除任何信息交换，除非用于诊断测试或表决目的？	0.5	0.5	0.5	0.5
设计时使用的技术，是否是基于在现场已成功使用 5 年或 5 年以上的设备中所采用的技术？	0.5	1.0	1.0	1.0
在相似的环境中使用相同的硬件的经验是否已超过 5 年？	1.0	1.5	1.5	1.5
系统是否简单？如每个通道的输入/输出不大于 10。		1.0		
输入和输出是否具有可能级别的过压和过流的保护？	1.5	0.5	1.5	0.5
所有设备/部件是否经过适当的定额（例如，不小于 2）？	2.0		2.0	
评估/分析及数据反馈				
为建立共同原因失效源的失效模式、效果分析或故障树分析的结果是否已经通过测验，并且通过设计是否已经消除了事先确定了的共同原因失效源？		3.0		3.0
设计复审过程中，所考虑的共同原因失效的结果是否被反馈回设计中去了？（要求设计复审中的文档证据）		3.0		3.0
对现场失效的所有分析是否均反馈到设计中去了？（要求规程的文档证据）	0.5	3.5	0.5	3.5
规程/人工接口				
是否存在一种已书写的工作系统可以用来确保检测到的所有部件的失效（或老化）被记录？是否存在所建立的根本原因和用于检查类似潜在的失效原因的其他类似项目？		1.5	0.5	1.5
为保证独立通道中任一部分的维护（包括调节或校准）已升级，并且除在维护后执行手动检查外，在完成一个通道的维护与另一个通道开始进行维护之间允许满意地运行诊断测试的规程是否就位？	1.5	0.5	2.0	1.0
文档化的维护规程是否规定了冗余系统中所有部分（如电缆线等）之间是相互独立的，并不需重新定位？	0.5	0.5	0.5	0.5
是否所有印制电路板等的维护均需在质量维修中心工场外执行，而且，是否所有修复项目均通过了预装测试？	0.5	1.0	0.5	1.5

表 D.1（续）

项　　目	逻辑子系统		传感器和最终元件	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
系统是否为低诊断覆盖率(60%～90%)？并且是否对现场可置换模块层提供失效报告？	0.5			
系统是否为中等诊断覆盖率(90%～99%)？并且是否对现场可置换模块层提供失效报告？	1.5	1.0		
系统是否为高诊断覆盖率（>99%)？并且是否对现场可置换模块层提供失效报告？	2.5	1.5		
系统的诊断测试是否对现场可置换模块层提供了报告？			1.0	1.0
能力/培训/安全素养				
设计人员是否经过培训(使用培训文档)，从而懂得了共同原因失效的原因及后果？	2.0	3.0	2.0	3.0
维护人员是否经过培训(使用培训文档)，从而懂得了共同原因失效的原因及后果？	0.5	4.5	0.5	4.5
环境的控制				
人员的进出是否有限制(如上锁的机柜与不准许接近的位置)？	0.5	2.5	0.5	2.5
在无外部环境控制的情况下，系统是否总能在已经测试过的一定温度、湿度、腐蚀度、尘埃、振动等范围内工作？	3.0	1.0	3.0	1.0
信号和电源电缆在所有位置是否是隔离开的？	2.0	1.0	2.0	1.0
环境测试				
系统对所有有关环境的影响(如 EMC、温度、振动、冲击温度等)的抗干扰性是否达到认可的标准中规定的水平？	10.0	10.0	10.0	10.0

注 1：在设计阶段很难预测到与系统工作相关的许多项目。对于这些情况，设计者需要做出合理的假设，随后应保正系统最终用户能了解。例如为了达到安全完整性的设计水平，规程应该就位。在相伴的文档中，应包含必要的信息。

注 2：X、Y 列的值是根据工程判断得出的，并且考虑到了第 1 列中各项直接的与间接的影响，例如使用可现场替换模块会导致：

——制造商在受控条件下进行修理，而不是在不太合适的条件的现场进行(可能是错误的)修理。因为减小了系统失效(因此也减小了共同原因失效)的概率，从而对 Y 列作出了一定贡献；

——现场手动相互作用需要的减少以及可能在线快速更换故障模块的能力，提高了在失效变成共同原因失效之前识别它们的诊断效率。这在 X 列中产生了一个较大的值。

表 D.2　Z 的值：可编程电子

诊断覆盖率	诊断测试间隔		
	小于 1 min	1 min～5 min	大于 5 min
≥99%	2.0	1.0	0
≥90%	1.5	0.5	0
≥60%	1.0	0	0

表 D.3 Z 的值:传感器或最终元件

诊断覆盖率	诊断测试间隔			
	小于 2 h	2 h～2 d	2 d～7 d	大于 7 d
≥99%	2.0	1.5	1.0	0
≥90%	1.5	1.0	0.5	0
≥60%	1.0	0.5	0	0

注 1:如果统一采用表 D.1 中的分类目录,则此方法是最有效的。因此,极力推荐每类 X、Y 列中的总分不能小于 X、Y 总和的 1/20。例如如果(X+Y)的总分为 80,那么任何类(如规程/人工接口)的(X+Y)总和不小于 4。

注 2:当使用表 D.1 时,应考虑到所有应用项目的总分,允许对相互不排斥的项目设计评分。

例如:具有分离机柜的逻辑子系统通道的系统被赋予"逻辑子系统通道是否在各自的框架中?"和"逻辑子系统的所有通道的印制电路板是否是单独的?"两个分数。

注 3:如果传感器或最终元件是以 PE 为基础的,当把它们作为构成逻辑子系统的主要部分的设备,安放在同一建筑物(或车辆)内时,则被视为逻辑子系统的一部分。否则,就应被视为传感器或最终元件。

注 4:对于使用非零 Z 值,应确保在非同步共同原因失效影响所有通道之前受控设备进入安全状态。同时保证安全状态的持续时间小于所声明的诊断测试时间间隔。非零 Z 值仅在下列情况下才可被使用:

——检测到故障时,系统启动自动关机;或

——在第一次故障后,并不启动安全关机[9],而诊断测试能:

- 确定故障位置,能给故障定位;或者
- 发现任何后续故障时,继续将 EUC 置于安全状态;或者

——为了保证在声明的诊断测试间隔中,充分调查已揭露出的任何故障的起因,一个正式的工作系统已安装到位;并且:

- 如果故障可能导致共同原因失效,应立即关闭设备;或
- 在申明的诊断测试期间隔中,修复了有故障的通道。

注 5:工业过程中,在诊断测试间隔中发现故障时,像表 D.2 中所描述的那样关闭 EUC 控制系统似乎是不太容易的。这种方法不应被曲解为:在发现这种故障时就要求关闭过程设备。但是,如果不实现关闭,对可编程电子使用诊断测试并不能降低 β 系数。在某些工业领域,在所描述的时间关闭是切实可行的。在这些情况下,就可能用到非零 Z 值。

注 6:在使用模块化方法执行诊断测试时,表 D.2 或表 D.3 中使用的重复时间是在连续完成整套模块的诊断测试之间的间隔时间。诊断覆盖率是由所有模块提供的总覆盖率。

表 D.4 β 和 β_D 的计算

得分(S 或 S_D)	β 或 β_D 的相应值	
	逻辑子系统	传感器或最终元件
不小于 120	0.5%	1%
70～120	1%	2%
45～70	2%	5%
小于 45	5%	10%
注 1:表中所示的 β_D 最大水平比平常使用中低,它反映了为了降低作为一个整体的系统失效的概率以及作为共同原因失效结果的共同原因失效的概率在 GB/T 20438 中其他地方所规定的技术的使用。 注 2:逻辑子系统中小于 0.5%的 β_D,传感器中小于 1%的 β_D 的合理性是很难证明的。		

9) 应考虑不同故障时系统的操作。例如,当识别出单一故障之后,表 D.2、表 D.3 中标出的时间内应关闭一个简单的 2oo3 系统。如果系统没有被关闭,第二通道的失效将使两个有故障的通道不表决其余的(正常的)通道。在一个通道出现故障时,可自动重新配置成 1oo2 表决的,并在第二通道出现故障时可自动关闭的系统,其揭露第二通道故障的概率将增大,所以可声明非零 Z 值。

D.7 方法使用的示例

为了演示使用此方法的效果，表 D.5 给出了一些已经完成的关于可编程电子的简单例子。

对于与多样性和冗余均无关的类别，使用了典型的 X 和 Y 值。

在多种系统示例中。多样性/冗余类别的值可以通过表 D.1 中所列的各项属性得出：

——其中一个系统为电子系统，其他的使用继电器技术；

——硬件诊断测试使用不同的技术；

——在设计过程中，不同的设计人员不进行交流；

——使用不同的测试方法和测试人员对系统进行试运行；并且

——在不同时间，由不同人员进行维护。

在冗余系统示例中，可通过独立系统使用同冗余系统中一样的技术，执行硬件诊断的属性得出多样性/冗余类别的值。

对多样性系统和冗余系统，使用 Z 的最大值和最小值，总共会产生 4 种示例系统。

表 D.5 可编程电子的示例值

类别		有良好诊断测试的多种系统	缺乏诊断测试的多种系统	拥有良好诊断测试的冗余系统	缺乏诊断测试的冗余系统
分离/隔离	X	3.50	3.50	3.50	3.50
	Y	1.50	1.50	1.50	1.50
多样性/冗余	X	14.50	14.50	2.00	2.00
	Y	3.00	3.00	1.00	1.00
复杂性/设计/……	X	2.75	2.75	2.75	2.75
	Y	2.25	2.25	2.25	2.25
评估/分析/……	X	0.25	0.25	0.25	0.25
	Y	4.75	4.75	4.75	4.75
规程/人工接口	X	3.50	3.50	3.50	3.50
	Y	3.00	3.00	3.00	3.00
胜任能力/培训/……	X	1.25	1.25	1.25	1.25
	Y	3.75	3.75	3.75	3.75
环境控制	X	2.75	2.75	2.75	2.75
	Y	2.25	2.25	2.25	2.25
环境测试	X	5.00	5.00	5.00	5.00
	Y	5.00	5.00	5.00	5.00
诊断覆盖率	Z	2.00	0.00	2.00	0.00
X 总计		33.5	33.5	21	21
Y 总计		25.5	25.5	23.5	23.5
S 得分		59	59	44.5	44.5
β		2%	2%	5%	5%
S_D 得分		126	59	86.5	44.5
β_D		0.5%	2%	1%	5%

D.8 参考

参考文献[10]～[12]提供了有关共同原因失效的有用信息。

附 录 E
（资料性附录）
GB/T 20438.3 中软件安全完整性表的应用示例

E.1 概述

此附录给出了 GB/T 20438.3—2006 附录 A 中规定的软件安全完整性表的应用中的两个工作示例。

第一个示例是化工厂生产过程所需的安全完整性等级 2 的一个可编程电子安全相关系统。可编程电子的应用程序使用了梯形逻辑，并且是应用有限可变语言编程的示例说明。

第二个示例是基于高级语言的安全完整性等级 3 的关机应用程序。

这两个工作示例为在不同环境中如何应用安全完整性表提供了指南。对于实系统应以文档支持表中所列的内容，以证明其正确性和对于具体的系统和应用有正确的响应。

E.2 安全完整性等级 2 的示例

这个例子中包括了几个反应容器，它们与一些中间贮存器相连，为了避免着火，引起爆炸，在反应周期中的固定点充入惰性气体。可编程电子安全相关系统的功能包括：按安全规范要求的那样接收传感器传来的输入信号；为阀门、泵、执行器供电，并将它们互锁；检测危险情况并启动报警；同分布式控制系统接口。

假设：

——可编程电子安全相关系统的控制器为一个 PLC；

——危险和风险分析已建立了在本应用中所需要的安全完整性等级为 2 的可编程电子安全相关系统（通过应用 GB/T 20438.1 和 GB/T 20438.2）；

——虽然控制器以实时方式工作，但仅需要相对较慢的响应；

——具有与操作人员和分布控制系统的接口；

——不便于对系统软件的源代码以及 PLC 可编程电子的设计进行考核，但已证实其能达到 GB/T 20438安全完整性等级 2；

——应用编程语言是梯形逻辑，它是由 PLC 供应商的开发系统产生的；

——要求应用代码仅在单一类型的 PLC 上运行；

——软件开发的全过程需要独立于软件开发小组的人进行复审；

——确认测试需要独立于软件开发小组的人在场和批准；

——修改（如果需要）要由独立于软件开发小组的人来授权。

注 1：有关独立的人的定义，见 GB/T 20438.4—2006 的 3.8.10。

表 E.1～表 E.10 通过本应用说明了 GB/T 20438.3—2006 附录 A。

注 2：下列表参考（名为 Ref）列中，技术和措施（例如 B.2.4，C.3.1）参考 GB/T 20438.7，表（如表 B.7）参考 GB/T 20438.3。

注 3：当使用有限可变编程时，有关供应商和用户之间责任的划分的信息可参见 GB/T 20438.3—2006 中 7.4.3、7.4.4、7.4.5 的注。

表 E.1 软件安全要求规范(见 GB/T 20438.3—2006 的 7.2)

技术/措施	Ref	SIL2	在本应用中的解释
1 计算机辅助规范工具	B.2.4	R	由 PLC 制造商提供的开发工具
2a 半形式化方法	表 B.7	R	因果图、时序图、功能块 典型地应用于 PLC 应用软件要求规范
3b 形式化方法包括 CCS、CSP、HOL、LOTOS、OBJ、时序逻辑、VDM、Z	C.2.4	R	不用于有限可变编程
注:用自然语言规定软件安全需求。			

表 E.2 软件设计与开发:软件结构设计(见 GB/T 20438.3—2006 的 7.4.3)

技术/措施	Ref	SIL2	在本应用中的解释
1 故障检测和诊断	C.3.1	R	检查数据范围、看门狗、输入/输出、通信出错时产生警报(见 3a)
2 差错检测和纠错码	C.3.2	R	嵌入有用户选项——要求仔细选择的
3a 失效断言编程	C.3.3	R	指定一些 PLC 程序梯形逻辑图以检测基本的安全条件
3b 安全包技术	C.3.4	R	在独立的硬件安全监视器中检查合法的输入/输出组合
3c 多种编程	C.3.5	R	应用要求的
3d 恢复程序块	C.3.6	R	嵌入有用户选项——要求仔细选择的
3e 反向恢复	C.3.7	R	嵌入有用户选项——要求仔细选择的
3f 正向恢复	C.3.8	R	嵌入有用户选项——要求仔细选择的
3g 重试故障恢复机制	C.3.9	R	根据应用中的需求使用
3h 存储执行用例	C.3.10	R	不用于有限可变编程中
4 功能退化	C.3.11	R	不用于有限可变编程中
5 人工智能故障纠正	C.3.12	NR	不用于有限可变编程中
6 动态再配置	C.3.13	NR	不用于有限可变编程中
7a 结构化方法包括:如 JSD、MASCOT、SADT 和 Yourdon	C.2.1	HR	至少可用数据流法及数据逻辑表来表示设计结构
7b 半形式化方法	表 B.7	R	可用于 DCS 接口
7c 形式化方法包括:如 CCS、CSP、HOL、LOTOS、OBJ、时序逻辑、VDM、Z	C.2.4	R	很少用于有限可变编程
8 计算机辅助规范工具	B.2.4	R	由 PLC 制造商提供的开发工具
注:在有限可变编程中实现某些上述技术是不切实际的。			

表 E.3 软件设计与开发:支持工具和编程语言(见 GB/T 20438.3—2006 的 7.4.4)

技术/措施	Ref	SIL2	在本应用中的解释
1 合适的编程语言	C.4.6	HR	通常采用梯形图,一般是 PLC 供应商的专有变种
2 强类型编程语言	C.4.1	HR	IEC 61121-3 结构化文档
3 语言子集	C.4.2	—	注意复杂的"宏"指令及中断,它们会改变 PLC 扫描周期等
4a 经认证的工具	C.4.3	HR	可从某些 PLC 供应商处买到
4b 工具:通过使用提高置信度	C.4.4	HR	PLC 供应商的开发工具包;经过几项工程开发的内部工具
5a 经认证的翻译器	C.4.3	HR	可从某些 PLC 供应商处买到
5b 翻译器:通过使用提高置信度	C.4.4	HR	不用于有限可变编程中
6 可信的经验证的软件模块和部件库	C.4.5	HR	功能块,部分程序

表 E.4 软件设计与开发:详细设计(见 GB/T 20438.3—2006 的 7.4.5 及 7.4.6)
(包括软件系统设计、软件模块设计和编码)

技术/措施	Ref	SIL2	在本应用中的解释
1a 结构化方法包括:JSD、MASCOT、SADT、Yourdon	C.2.1	HR	不用于有限可变编程中
1b 半形式化方法	表 B.7	HR	因果图、时序图、功能块 典型地用于有限可变编程
1c 形式化方法包括:CCS、CSP、HOL、LOTOS、OBJ、时序逻辑、VDM、Z	C.2.4	R	不用于有限可变编程中
2 计算机辅助设计工具	B.3.5	R	由 PLC 制造商提供的开发工具
3 防御性编程	C.2.5	R	包括在系统软件中
4 模块法	表 B.9	HR	将 PLC 程序梯形逻辑排序和分组,达到功能要求的最大模块化所要求的
5 设计和编码标准	表 B.1	HR	内部文档化及可维护性的内部约定
6 结构化编程	C.2.7	HR	与文中模块化类似
7 使用可信的/经验证的软件模块及部件(若可获得)	C.4.5	HR	被使用

表 E.5 软件设计与开发:软件模块测试和集成(见 GB/T 20438.3—2006 的 7.4.7 及 7.4.8)

技术/措施	Ref	SIL2	在本应用中的解释
1 概率测试	C.5.1	R	不用于有限可变编程中
2 动态分析和测试	B.6.5 表 B.2	HR	被使用
3 数据记录和分析	C.5.2	HR	测试用例及结果的记录

表 E.5（续）

技术/措施	Ref	SIL2	在本应用中的解释
4 功能和黑盒测试	B.5.1 B.5.2 表 B.3	HR	选择输入数据以便演习所有规定的功能用例，包括错误处理测试用例来自因果图、边界值分析，以及输入划分
5 性能建模	C.5.20 表 B.6	R	不用于有限可变编程
6 界面测试	C.5.3	R	包括在功能和黑盒测试中

表 E.6 可编程电子集成（硬件和软件）（见 GB/T 20438.3—2006 的 7.5）

技术/措施	Ref	SIL2	在本应用中的解释
1 功能和黑盒测试	B.5.1 B.5.2 表 B.3	HR	选择输入数据以便演习所有规定的功能用例，包括错误处理。测试用例来自因果图、边界值分析，以及输入划分
2 性能测试	C.5.20 表 B.6	R	用于装配 PLC 系统时工厂验收测试

表 E.7 软件安全确认（见 GB/T 20438.3—2006 的 7.7）

技术/措施	Ref	SIL2	在本应用中的解释
1 概率测试	C.5.1	R	不用于有限可变编程中
2 仿真/建模	表 B.5	R	不用于有限可变编程，但在 PLC 系统开发中应用更普遍
3 功能和黑盒测试	B.5.1 B.5.2 表 B.3	HR	选择输入数据以便演习所有规定的功能用例，包括错误处理。测试用例来自因果图、边界值分析，以及输入划分

表 E.8 软件修改（见 GB/T 20438.3—2006 的 7.8）

技术/措施	Ref	SIL2	在本应用中的解释
1 影响分析	C.5.23	HR	执行影响分析以便考虑整个系统模块化如何限制所提出的改变产生的影响
2 重新验证被改变的软件模块	C.5.23	HR	重复前面的测试
3 重新验证受到影响的软件模块	C.5.23	HR	重复前面的测试
4 重新确认整个系统	C.5.23	R	影响分析显示出修改是必要的，因此根据要求进行重新确认
5 软件配置管理	C.5.24	HR	基线，改变记录，对其他系统的影响要求
6 数据记录和分析	C.5.2	HR	测试用例和结果的记录

表 E.9 软件验证(见 GB/T 20438.3—2006 的 7.9)

技术/措施	Ref	SIL2	在本应用中的解释
1 形式化检验	C.5.13	R	不用于有限可变编程中
2 概率测试	C.5.1	R	以现有部分的操作经验代替
3 静态分析	B.6.4 表 B.8	HR	变量、条件等使用的书面交叉引用
4 动态分析和测试	B.6.5 表 B.2	HR	用于回归测试的自动化测试装置
5 软件复杂性度量	C.5.14	R	不用于有限可变编程中
软件模块测试和集成	见表 E.5		
可编程电子集成测试	见表 E.6		
软件系统测试(确认)	见表 E.7		

表 E.10 功能安全评估(见 GB/T 20438.3—2006 的第 8 章)

技术/措施	Ref	SIL2	在本应用中的解释
1 检查表	B.2.5	R	被使用
2 判定/真值 表	C.6.1	R	用于有限水平中
3 软件复杂性度量	C.5.14	R	不用于有限可变编程中
4 失效分析	表 B.4	R	在系统层使用因果图,但是对于有限可变编程的其他方面,不使用失效分析
5 多种软件的共同原因失效分析(如果使用多种软件时)	C.6.3	R	不用于有限可变编程中
6 可靠性块图	C.6.5	R	不用于有限可变编程中

E.3 安全完整性等级 3 的示例

就安全相关系统而言,软件系统是比较大的;特别为系统开发的源代码就有 30 000 多行,还使用了常用的固有功能——至少两种不同的操作系统和早期工程项目中预存在的代码(已使用证实的),总而言之,如果这些都可获得,系统由 100 000 多行源代码构成。

整个硬件(包括传感器和执行器)是一个双通道系统,其对最终元件的输出被连接成逻辑与(AND)。

假设:

——虽然不需要快速响应,但是要保证最大的响应时间;

——具有操作人员到传感器、执行器和信号器的接口;

——得不到操作系统的源代码、图形例程、商业数学例程;

——系统很可能有进一步的改变;

——使用一种通用规程语言来开发一些特殊软件;

——系统是部分面向对象的;

——不能得到源代码的所有部分要通过不同供应商提供的软件部件分别实现,并且它们的对象代码要由不同翻译器生成;

——软件可在几个能满足 GB/T 20438.2 要求的且在市场上可获得的处理器上运行；

——GB/T 20438.2 关于控制和避免硬件故障的所有要求均由嵌入式系统来满足；

——软件的开发由独立组织进行评估。

注 1：关于独立组织的定义见 GB/T 20438.4—2006 的 3.8.12。

表 E.11～表 E.20 通过本应用说明了 GB/T 20438.3—2006 的附录。

注 2：下列表参考(名为 Ref)列中，技术和措施(例如 B.2.4，C.3.1)参考 GB/T 20438.7，表(如表 B.7)参考 GB/T 20438.3。

表 E.11 软件安全要求规范(见 GB/T 20438.3—2006 的 7.2)

技术/措施	Ref	SIL3	在本应用中的解释
1 计算机辅助规范工具	B.2.4	HR	支持已选方法的工具
2a 半形式化方法	表 B.7	HR	块图、时序图、状态转换图
2b 形式化方式包括：CCS，CSP，HOL，LOTOS，OBJ，时序逻辑，VDM，Z	C.2.4	R	仅在特殊情况下使用

表 E.12 软件设计与开发：软件结构设计(见 GB/T 20438.3—2006 的 7.4.3)

技术/措施	Ref	SIL3	在本应用中的解释
1 故障检测和诊断	C.3.1	HR	涉及传感器、执行器、数据传输失效，以及那些根据 GB/T 20438.2 的要求，在嵌入式系统内的措施未覆盖的失效
2 差错检测及纠错码	C.3.2	R	仅用于外部数据传输
3a 失效断言编程	C.3.3	R	对应用功能的结果进行有效性检查
3b 安全包技术	C.3.4	R	在 8a、3c 不被使用时，用于某些安全功能
3c 多种编程	C.3.5	R	在源代码得不到时，用于某些安全功能
3d 恢复程序块	C.3.6	R	不使用
3e 反向恢复	C.3.7	R	不使用
3f 正向恢复	C.3.8	R	不使用
3g 重试故障恢复机制	C.3.9	R	不使用
3h 存储执行用例	C.3.10	R	不使用(3a、3b、3c 的措施就足够了)
4 功能退化	C.3.11	HR	是的，因为工艺过程的固有特性
5 人工智能-故障纠正	C.3.12	NR	不使用
6 动态再配置	C.3.13	NR	不使用
7a 结构化方法包括：JSD、MASCOT、SADT、Yourdon	C.2.1	HR	需要，视系统的规模而定
7b 半形式化方法	表 B.7	HR	块图、时序图、状态转换图
7c 形式化方式包括：CCS，CSP，HOL，LOTOS，OBJ，时序逻辑，VDM，Z	C.2.4	R	不使用
8 计算机辅助规范工具	B.2.4	HR	支持所选方法的工具

表 E.13 软件设计与开发:支持工具及编程语言(见 GB/T 20438.3—2006 的 7.4.4)

技术/措施	Ref	SIL3	在本应用中的解释
1 合适的编程语言	C.4.6	HR	选择的全可变高级语言
2 强类型编程语言	C.4.1	HR	已使用
3 语言子集	C.4.2	HR	为选择的语言定义子集
4a 经认证的工具	C.4.3	HR	不可得到
4b 工具:通过使用提高置信度	C.4.4	HR	可得到,并已使用
5a 经认证的翻译器	C.4.3	HR	不可得到
5b 翻译器:通过使用提高置信度	C.4.4	HR	可得到,并在使用中
6 可信任的/经验证的软件模块和部件库	C.4.5	HR	可得到,并已使用

表 E.14 软件设计与开发:详细设计(见 GB/T 20438.3—2006 的 7.4.5 和 7.4.6)
(包括软件系统设计、软件模块设计和编码)

技术/措施	Ref	SIL3	在本应用中的解释
1a 结构化方法包括 JSD, MASCOT, SADT, Yourdon	C.2.1	HR	广泛使用,特别是 SADT、JSD
1b 半形式化方法	表 B.7	HR	有限状态机/状态转换图、块图、时序图
1c 形式化方法包括 CCS, CSP, HOL, LOTOS, OBJ, 时序逻辑, VDM, Z	C.2.4	R	仅针对一些基本的元件,在特殊情况下才使用
2 计算机辅助设计工具	B.3.5	HR	用于所选择的方法
3 防御性编程	C.2.5	HR	除了编译器自动插入的那些措施外,所有措施均在它们有效的场合下被使用在应用软件中
4 模块法	表 B.9	HR	软件模块大小的限制,信息隐蔽/封装,在子程序中设置单入口/单出口以及相关功能,充分定义的接口……
5 设计和编码标准	表 B.1	HR	使用编码标准,无动态对象,无动态变量,有限地使用中断,有限地使用指针,有限地使用递归,不使用无条件跳转
6 结构化编程	C.2.7	HR	已被使用
7 使用可信任的/经验证的软件模块和部件库(如可得到)	C.4.5	HR	可得到并已使用

表 E.15 软件设计与开发:软件模块测试和集成(见 GB/T 20438.3—2006 的 7.4.7 和 7.4.8)

技术/措施	Ref	SIL3	在本应用中的解释
1 概率测试	C.5.1	R	在得不到源代码、以及难于定义测试数据的边界值和等价类时可使用于软件模块
2 动态分析及测试	B.6.5 表 B.2	HR	在得不到源代码时可用于软件模块;测试用例来自边界值分析,性能建模,等价类和输入划分和基于结构的测试

表 E.15（续）

技术/措施	Ref	SIL3	在本应用中的解释
3 数据记录和分析	C.5.2	HR	测试用例及结果的记录
4 功能和黑盒测试	B.5.1 B.5.2 表 B.3	HR	在得不到源代码时用于软件模块测试及集成测试 选择输入数据，以便演习所有功能用例（包括错误处理） 测试用例来自因果图、原型设计、边界值分析、等价类和输入划分
5 性能建模	C.5.20 表 B.6	HR	在对目标硬件进行集成测试时使用
6 界面测试	C.5.3	HR	未使用

表 E.16 可编程电子集成（硬件和软件）（见 GB/T 20438.3—2006 的 7.5）

技术/措施	Ref	SIL3	在本应用中的解释
1 功能和黑盒测试	B.5.1 B.5.2 表 B.3	HR	作为软件集成检测的附加测试（见表 E.15）使用 选择输入数据，以便演习规定的所有功能用例（包括错误处理） 测试用例来自因果图、原型设计、边界值分析、等价类和输入划分
2 性能建模	C.5.20 表 B.6	HR	被广泛地使用

表 E.17 软件安全确认（见 GB/T 20438.3—2006 的 7.7）

技术/措施	Ref	SIL3	在本应用中的解释
1 概率测试	C.5.1	R	未被用来确认
2 仿真/建模	表 B.5	HR	有限状态机，性能建模，原型设计和动画
3 功能和黑盒检测试	B.5.1 B.5.2 表 B.3	HR	选择输入数据，以便演习所有规定的功能用例（包括错误处理） 测试用例来自因果图、边界值分析、输入划分

表 E.18 修改（见 GB/T 20438.3—2006 的 7.8）

技术/措施	Ref	SIL3	在本应用中的解释
1 影响分析	C.5.23	HR	已被使用
2 重新验证被改变的软件模块	C.5.23	HR	已被使用
3 重新验证受到影响的软件模块	C.5.23	HR	已被使用
4 重新确认整个系统	C.5.23	HR	根据影响分析的结果
5 软件配置管理	C.5.24	HR	已被使用
6 数据记录和分析	C.5.2	HR	已被使用

表 E.19 软件的确认(见 GB/T 20438.3—2006 的 7.9)

技术/措施	Ref	SIL3	在本应用中的解释
1 形式化证实	C.5.13	R	仅在特殊情况下,供一些基本的类型使用
2 概率测试	C.5.1	R	包含于表 E.15 中
3 静态分析	B.6.4 表 B.8	HR	对于所有最新开发的代码,边界值分析,检查表,控制流分析、数据流分析、Fagan 检查法,设计复审
4 动态分析和测试	B.6.5 表 B.2	HR	包括在表 E.15 中
5 软件复杂性度量	C.5.14	R	仅有少量使用
软件模块测试和集成	见表 E.15		
可编程电子集成测试	见表 E.16		
软件系统测试(确认)	见表 E.17		

表 E.20 功能安全评估(见 GB/T 20438.3—2006 的第 8 章)

技术/措施	Ref	SIL3	在本应用中的解释
1 检查表	B.2.5	R	已被使用
2 判定/真值 表	C.6.1	R	有限地使用
3 软件复杂性度量	C.5.14	R	仅有少量使用
4 失效分析	表 B.4	HR	故障树分析被广泛地使用;因果图也被有限地使用
5 多种软件的共同原因失效分析(当多种软件在实际使用时)	C.6.3	HR	已被使用
可靠性块图	C.6.5	R	已被使用

参 考 文 献

下列参考文献给出了评价失效概率(见附录 B)的更多详情：

[1] IEC 61078:1991 可靠性分析技术 可靠性方框图方法.

[2] IEC 61165:1995 马尔可夫(Markov)技术.

[3] BS5760 系统设备和部件的可靠性 第 2 部分:可靠性评估指南.

[4] D·J·Smith. 可靠性、可维性和风险——工程师的实际方法. Butterworth-Heinemann. 5thed,1997.

[5] R·Billington and R·N·Allan. 工程系统的可靠性评价. Plenum,1992.

[6] W·W·Godble. 评价控制系统的可靠性——技术和应用. Instrument Society of America,1992.

计算诊断复盖率(见附录 C)可参考的文献包括：

[7] 可靠性分析中心(RAC). 失效模式/机制分配,1991.

[8] Qualität und Zuverlassigkeit technischer Systeme, Theoric, Praxis, Management. Dritte Auflage, 1991, Allessandro Birolini, Springer-Verlag Berlin Heidelberg New York.

[9] MIL-HDBK-217F. 电子设备可靠性预测军用手册,2 Dec. 1991,美国国防部.

以下参考文献提供了共同原因失效(见附录 D)的有关信息：

[10] 安全应用中的可编程电子系统第 2 部分:总的技术指南. Health and Safety Executive, HMSO, 1987.

[11] 给 β 系数共同原因评价分配一个数值. Humphreys, R·A·, Proc. Reliability'87.

[12] UPM3.1 标准系统相关失效评价的一种实用方法. AEA Technology, Report SRDA-R-13,1996.

表 E.3 中引用了下列标准：

[13] IEC 61131-3:1993 可编程控制器 第 3 部分:编程语言.

[14] ANSI/ISA S84.01:1996 过程工业领域安全仪表系统的应用.

GB/T 20438.6—2006/IEC 61508-6:2000

中 华 人 民 共 和 国
国 家 标 准
电气/电子/可编程电子安全相关系统的
功能安全 第6部分:GB/T 20438.2和
GB/T 20438.3的应用指南
GB/T 20438.6—2006/IEC 61508-6:2000
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 4 字数 124千字
2007年2月第一版 2007年2月第一次印刷
*
书号:155066·1-28712 定价 27.00 元

GB/T 20438.6-2006