ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.6—2017/IEC 61508-6:2010
代替 GB/T 20438.6—2006

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 61508-6:2010,Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 6:Guidelines on the application of IEC 61508-2 and IEC 61508-3,IDT)

2017-12-29 发布　2018-07-01 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

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—2017/IEC 61508-6:2010
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2017年11月第一版
*
书号:155066·1-57856

目　　次

前　言

GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》分为七个部分：

——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。

本部分为GB/T 20438的第6部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 20438.6—2006《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》，与GB/T 20438.6—2006相比，主要技术变化如下：

——增加了评估硬件失效概率的方法，如故障树、马尔科夫模型、佩特里网等(见附录B)；

——增加了不同结构共因失效因子的方法(见附录D.7)。

本部分使用翻译法等同采用IEC 61508-6:2010《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》。

本部分做了下列编辑性修改：

——为与现有标准系列一致，将标准名称改为《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》

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控制和自动化标准化技术委员会(SAC/TC 124)归口。

本部分起草单位：机械工业仪器仪表综合技术经济研究所、北京国电智深控制技术有限公司、北京和利时系统工程有限公司、上海黑马安全自动化系统有限公司、皮尔磁工业自动化贸易(上海)有限公司、横河电机(中国)有限公司、上海工业自动化仪表研究院、上海中沪电子有限公司、西门子(中国)有限公司。

本部分主要起草人：史学玲、熊文泽、潘钢、杨柳、黄之炯、李佳嘉、周有铮、姜雪莲、钱大涛、冯晓升、罗安、李佳、刘晓东、方来华、田雨聪、顾峥、鲁毅、梅豪、许鹏、申弢。

本部分所代替标准的历次版本发布情况为：

——GB/T 20438.6—2006。

引　言

由电气和电子器件构成的系统，多年来在许多应用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）在其应用领域中用于执行非安全功能，并且也越来越多地用于执行安全功能。如果要安全并有效地使用计算机技术，有关决策者在安全方面有充足的指导并据此做出决定是十分必要的 。

GB/T 20438 针对由电气和/或电子和/或可编程电子（E/E/PE）组件构成的、用来执行安全功能的系统安全生命周期的所有活动，提出了一个通用的方法。采用统一的方法的目的是为了针对所有以电为基础的安全相关系统提出一种一致的、合理的技术方针。主要目标是促进基于 GB/T 20438 系列标准的产品和应用领域国家标准的制定。

注 1：在参考文献中给出了基于 GB/T 20438 系列标准的产品和应用领域标准的例子（见参考文献[1]，[2]，[3]）。

在许多情况下，可用多种基于不同技术（如机械的、液压的、气动的、电气的、电子的、可编程电子的等）的系统来保证安全。因而不得不考虑各类安全策略，不仅要考虑单个系统中的所有组件的问题（如传感器、控制器、执行器等），还要考虑不同安全相关系统组合后的问题。因此当 GB/T 20438 在关注电气/电子/可编程电子（E/E/PE）安全相关系统的同时，也提供了一个框架，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/PE 安全相关系统。对每个特定的应用，根据特定应用的许多因素来确定所需的安全措施。GB/T 20438 作为基本原则可在未来的产品和应用领域国家标准制定和已有标准的修订中规范这些措施。

GB/T 20438

——考虑了当使用 E/E/PE 系统执行安全功能时，所涉及的整体安全生命周期、E/E/PE 系统安全生命周期以及软件安全生命周期的各阶段（如初始概念、整体设计、实现、运行和维护到退役）；

——针对飞速发展的技术，建立一个足够健全且广泛满足未来发展需求的框架；

——使涉及 E/E/PE 安全相关系统的产品和应用领域的国家标准得以制定；在 GB/T 20438 的框架下，产品和应用领域的国家标准的制定在应用领域和交叉应用领域具有高度一致性（如基本原理，术语等）；这将既具有安全性又具有经济效益；

——为实现 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；

——采用了一种可确定安全完整性要求的基于风险的方法；

——引入安全完整性等级，用于规定 E/E/PE 安全相关系统所要执行的安全功能的目标安全完整性等级；

注 2：GB/T 20438 没有规定每个安全功能的安全完整性等级的要求，也没有规定如何确定安全完整性等级。而是提供了一种基于风险概念的框架和技术范例。

——建立了 E/E/PE 安全相关系统执行安全功能的目标失效量，这些量都同安全完整性等级相联系；

——建立了单一 E/E/PE 安全相关系统执行安全功能时，目标失效量的一个下限值；这些 E/E/PE 安全相关系统运行在：

——低要求运行模式下，下限设定成要求时危险失效平均概率为 10^{-5}；

——高要求或连续运行模式下，下限设定成危险失效平均频率为 10^{-9}/h。

注 3：单一 E/E/PE 安全相关系统不一定是单通道架构。

注 4：对于非复杂系统，通过安全相关系统的设计实现更优目标安全完整性是可能的。但对于相对复杂的系统（例如可编程电子安全相关系统），这些限值代表了目前能够达到的水平。

——基于工业实践中获取的经验和判断，设定了避免和控制系统性故障的要求；即使发生系统性故障的可能性一般不能量化，但 GB/T 20438 允许为一个特定的安全功能做出声明，即如果标准中的所有要求都满足，认为与安全功能相关的目标失效量已达到；

——引入了系统性能力，该能力表明一个组件为满足规定的安全完整性等级要求时，系统性安全完整性的置信度；

——采用多种原理、技术和措施以实现 E/E/PE 安全相关系统的功能安全，但没有明确地使用失效-安全的概念。然而，如果能够满足标准中相关条款的要求，则“失效-安全”的概念和“本质安全”原则可能被应用，并且采用这些概念是可接受的。

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　GB/T 20438的本部分包括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—2017的7.4.3、附录C和本部分的附录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—2017的附录C。

——附录D阐述了将硬件共因失效率量化的方法。

——附录E给出了GB/T 20438.3—2017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是基础的安全标准,虽然它不适用于低复杂的E/E/PE安全相关系统(见GB/T 20438.4—2017的3.4.3),但作为基础安全标准,各技术委员会可以在IEC指南104和ISO/IEC指南51的指导下制定相关标准时使用。GB/T 20438.1、GB/T 20438.2、GB/T 20438.3和GB/T 20438.4也可作为独立标准来使用。GB/T 20438的横向安全功能不适用于在IEC 60601系列指导下的医疗设备。

1.3　技术委员会的职责之一就是只要合适,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表示了GB/T 20438的整体框架,同时明确了本部分在实现E/E/PE安全相关系统功能安全过程中的作用。

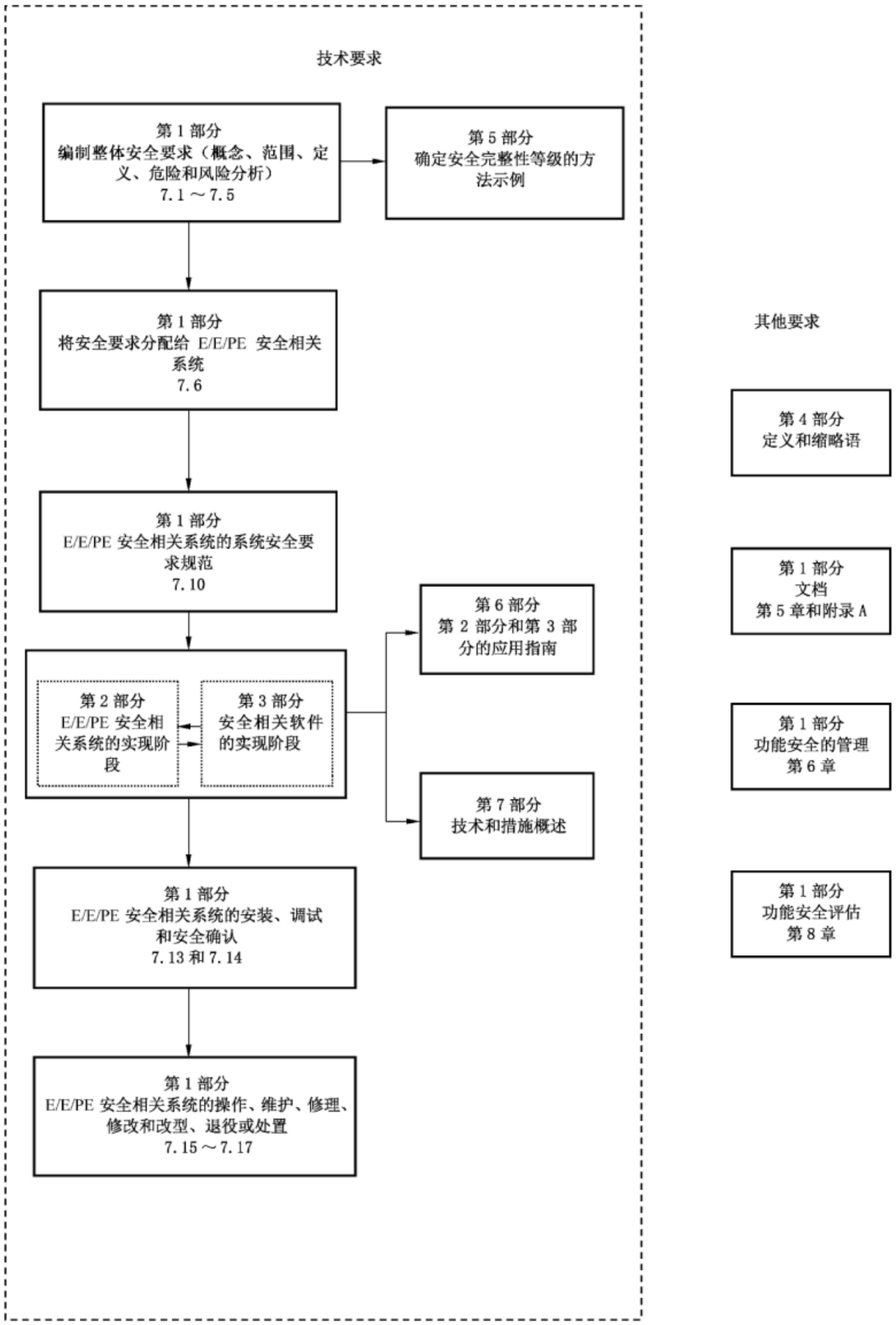


图 1　GB/T 20438 的整体框架

2 规范性引用文件

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

GB/T 20438.2—2017 电气/电子/可编程电子安全相关系统的功能安全 第2部分：电气/电子/可编程电子安全相关系统的要求(IEC 61805-2:2010，IDT)

GB/T 20438.3—2017 电气/电子/可编程电子安全相关系统的功能安全 第3部分：软件要求(IEC 61508-3:2010，IDT)

GB/T 20438.4—2017 电气/电子/可编程电子安全相关系统的功能安全 第4部分：定义和缩略语(IEC 61508-4:2010，IDT)

3 定义和缩略语

GB/T 20438.4—2017 界定的定义和缩略语适用于本文件。

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、工艺装置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、机械卷入等危险事件，对人员和环境产生一定风险。失效既可能因设备的物理故障（如引起随机硬件失效），也可能因为系统性故障（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导致的系统性失效）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整体框架，用于防止和/或控制机电、电子或者可编程电子设备中的失效。

GB/T 20438 的总目标就是确保装置和设备安全地自动运行，其中关键目标就是防止：

——控制系统性失效触发其他事件，继而可能导致（火灾、有毒物质泄漏、机械设备反复冲击等）危险；以及

——保护系统（如紧急停车系统）中未检测到的失效，这些失效使系统不能在需要时正常执行安全动作。

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。风险基于对危险事件的后果（或严重性）和频率（或概率）的评估。

GB/T 20438.1 进一步要求由风险分析得到的风险降低量，来确定是否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/或控制随机硬件失效和系统性失效（E/E/PE 系统和软件安全生命周期[3]）。

GB/T 20438.2 和 GB/T 20438.3 并没有给出针对指定的可容忍风险要求，哪一级安全完整性合适的指南。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]，这些措施与技术可按安全完整性进行分级，作为预防性方法用于避免系统性失效[5]。

——利用故障检测、冗余和架构特性（如多样性）等设计特性来控制系统性失效（包括软件失效）和

1） 功能安全所需要的系统包含一个或多个电气（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，还包括所有执行安全功能所必需的设备（见 GB/T 20438.4—2017 的 3.4.1）。

2） 安全完整性规定为四个不同的等级。安全完整性等级 4 为最高，安全完整性等级 1 为最低（见 GB/T 20438.1—2017 的 7.6.2.9）。

3） 为了清晰地说明 GB/T 20438 的要求，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—2017 的第 6 章）。

4） 在 GB/T 20438.2—2017 和 GB/T 20438.3—2017 的附录 A 和附录 B 的表中给出了每一个安全完整性等级所需的技术和措施。

5） 系统性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缺陷；考虑环境（如温度）引起的失效，以及操作相关的失误（如界面不友好）。

随机硬件失效。

在 GB/T 20438.2 中，对于危险随机硬件失效，保证安全完整性目标得以满足是基于：

——硬件故障裕度要求（见 GB/T 20438.2—2017 的表 2、表 3）；并且

——子系统与部件的诊断覆盖率和检验测试的频率，通过使用适当的数据执行一次可靠性分析。

在 GB/T 20438.2 与 GB/T 20438.3 中，满足系统性失效要求的安全完整性目标，可通过以下获得：

——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]；

——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性失误，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）达到安全完整性提出要求。应使用技术和措施防止随机性硬件失效和系统性硬件失效。如上所述，它们包括适当的措施以避免故障和控制失效。对于功能安全需要人员动作的情况，给出了操作员界面的要求。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（例如多样性）的诊断测试技术和措施。

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出要求。由于还不知道何种方法可证明适度复杂的安全相关软件中不存在故障，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）和故障裕度方法的组合（软件架构）。GB/T 20438.3 需要采用如下软件工程原则：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、便于验证和确认的清晰文档。不同级别的软件需要不同级别的保证，以确保这些以及相关原则得以正确应用。

软件开发者与整个 E/E/PE 系统的开发组织可独立也可不独立。无论哪种情况，密切协作都是必要的，特别是在可编程电子的架构开发中，需要从安全效果出发考虑硬件和软件架构之间的折中方案（见 GB/T 20438.2—2017 的图 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/PE 系统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/PE 系统的安全要求，包括安全完整性要求（见 GB/T 20438.2—2017 的 7.2）。给软件分配要求并提交给软件供应商和/或开发者以便应用 GB/T 20438.3。

注 1：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失效的概率（见 GB/T 20438.1—2017 的 7.5.2.4）。它们可能是由于例如受相似环境影响的共因失效的部件所引起。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处理。

c) 启动 E/E/PE 安全确认计划编制阶段（见 GB/T 20438.2—2017 的 7.3）。

d) 规定 E/E/PE 逻辑子系统、传感器和最终元件的架构（配置）。与软件供应商/开发者一起复

6) 如果在编制安全计划过程中已将合理性证明归档，那么 GB/T 20438 中规定的那些措施可以被替代（见 GB/T 20438.1—2017 的第 6 章）。

7) 独立评估不一定是第三方评估（见 GB/T 20438.1—2017 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。

审硬件和软件架构以及硬件和软件之间折衷方案的安全影响(见 GB/T 20438.2—2017 的图 4)。如果需要将重复此步骤。

e) 开发 E/E/PE 安全相关系统硬件架构模型,通过分别检查每个安全功能来开发架构模型并确定用来执行这些功能的子系统(元器件)。

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

——失效的检验测试时间间隔,这些失效是不会自动检测到的;

——平均恢复时间;

——诊断覆盖率(见 GB/T 20438.2—2017 的附录 C);

——失效概率;

——要求的架构约束;路径 1_H 见 GB/T 20438.2—2017 的 7.4.4.2 和附录 C,路径 2_H 见 GB/T 20438.2—2017 的 7.4.4.3。

g) 为 E/E/PE 安全相关系统所要执行的每一个安全功能建立可靠性模型。

注 2:可靠性模型是一个数学公式,用于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。

h) 使用适当的技术计算每个安全功能的可靠性预测值,将上面 b)项中确定的目标失效量结果同路径 1_H(见 GB/T 20438.2—2017 的 7.4.4.2)或路径 2_H(见 GB/T 20438.2—2017 的 7.4.4.3)的要求进行比较。如果预测的可靠性与目标失效量不同和/或不符合路径 1_H 或路径 2_H 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

——改变硬件架构(返回到上面的 d))。

注 3:有多种建模方法,分析人员宜选择最适合的方法(见附录 B 可使用方法的指南)

i) 进行 E/E/PE 安全相关系统的设计。选择用于控制系统性硬件失效、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—2017 的附录 A)。

j) 在目标硬件上集成(见 GB/T 20438.2—2017 的 7.5 及附录 B)经验证过的软件(见 GB/T 20438.3),同时为用户和维护人员制定系统操作规程(见 GB/T 20438.2—2017 的 7.6 及附录 B)。包括软件方面(见附录 A 中 A.3 f))。

k) 与软件开发者(见 GB/T 20438.3—2017 的 7.7)一起确认 E/E/PE 系统(见 GB/T 20438.2—2017 的 7.7 和附录 B)。

l) 把硬件和 E/E/PE 安全相关系统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。

m) 如果在使用寿命期限内需要维护或修改 E/E/PE 安全相关系统,则将适当的重新采用 GB/T 20438.2 (见 GB/T 20438.2—2017 的 7.8)。

用 GB/T 20438.2(见 GB/T 20438.2—2017 的 7.8)。在整个 E/E/PE 安全相关系统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—2017 的 7.9)和功能安全评估(见 GB/T 20438.1—2017 的第 8 章)。

在应用上述步骤的时候,应选择 E/E/PE 安全相关系统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(见 GB/T 20438.2—2017 的附录 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—2017 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 4:在应用上述步骤时如果在编制安全计划过程中已经建立合理性证明文档,那么 GB/T 20438 中规定的措施可以被替代(见 GB/T 20438.1—2017 的第 6 章)。

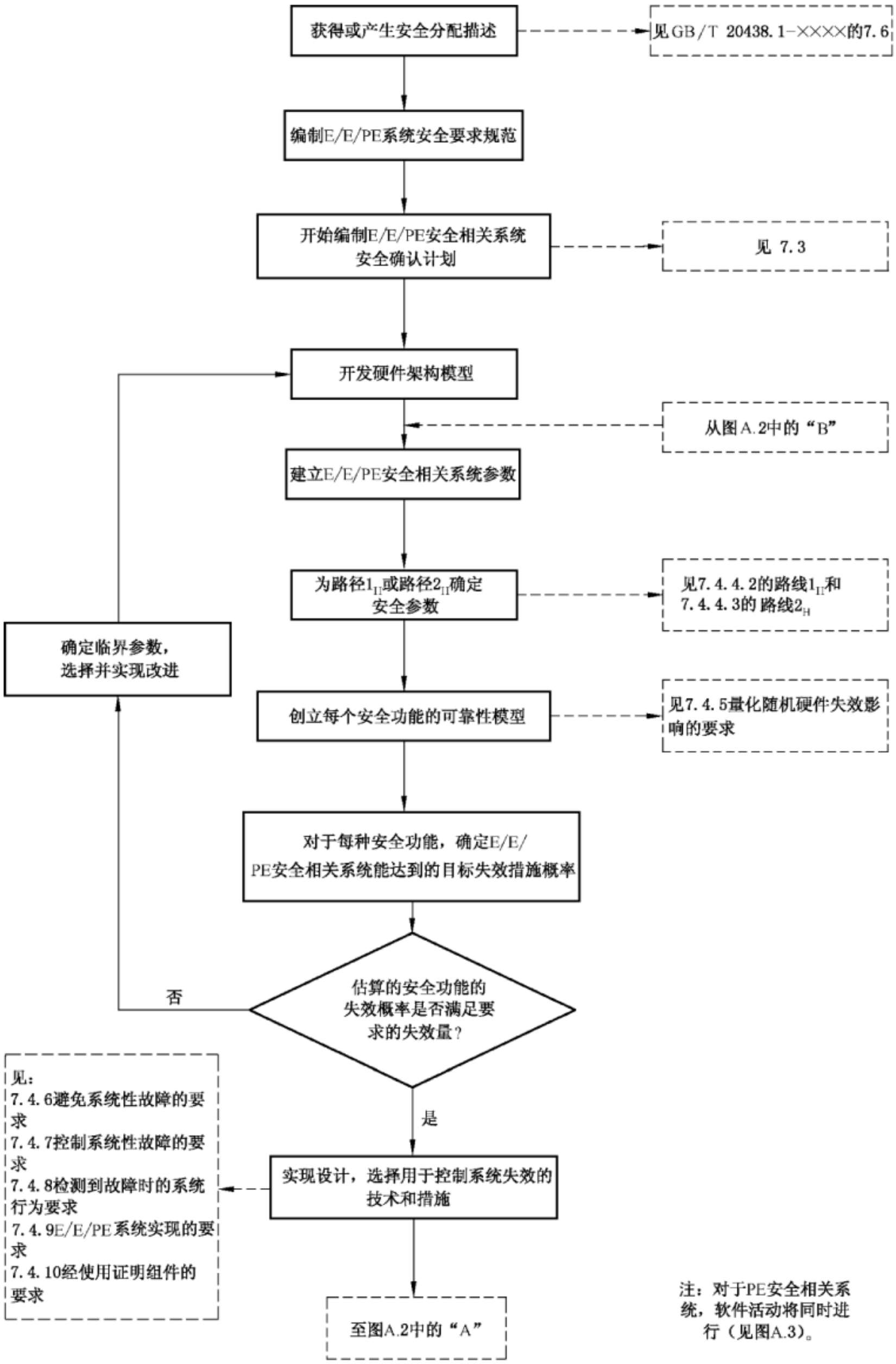


图 A.1 GB/T 20438.2 的应用

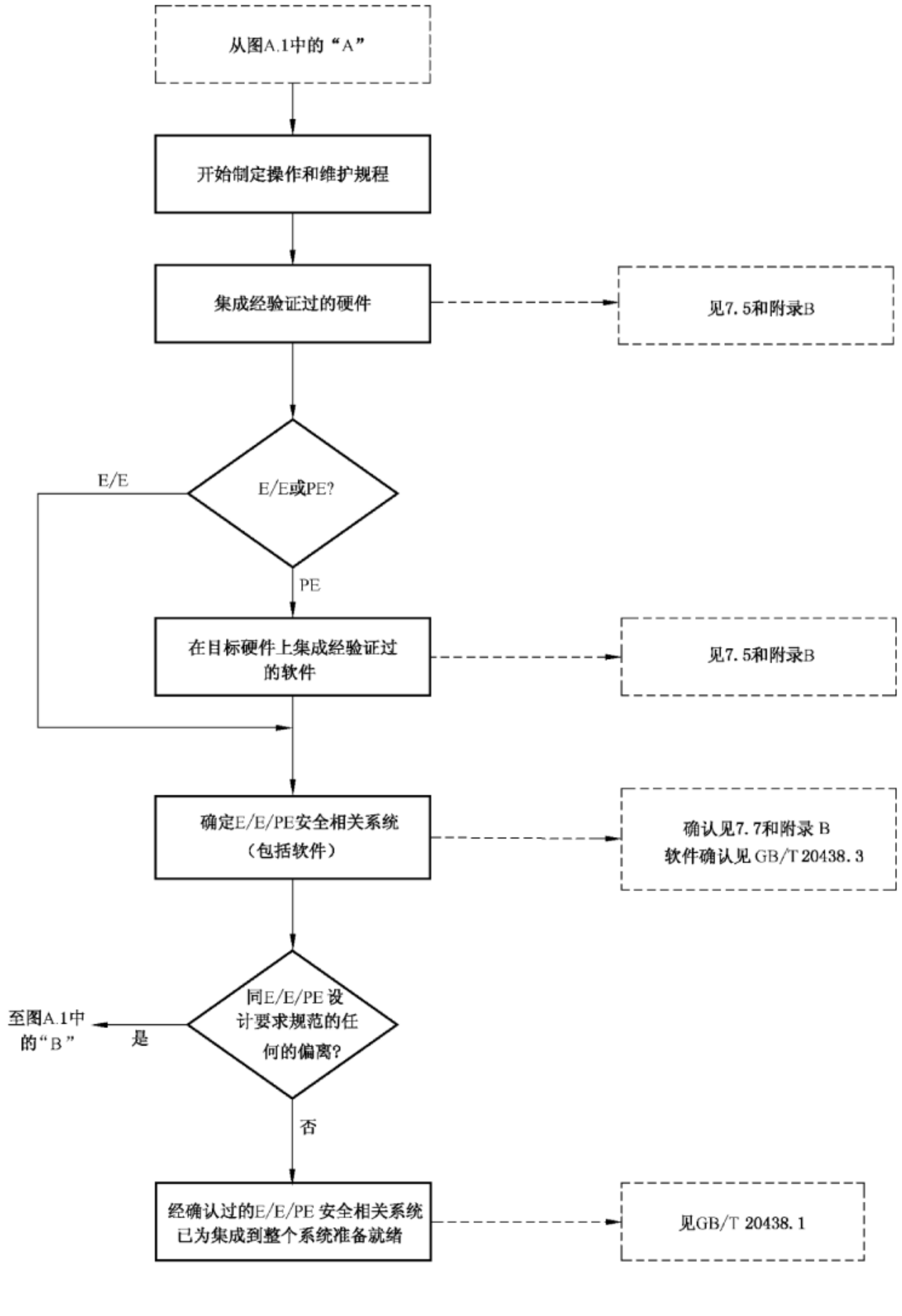


图 A.2　GB/T 20438.2 的应用（图 A.1 续）

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 20438.2—2017 的 7.3)。在开发软件期间,如必要时更新安全计划。

注 1:生命周期早期阶段已经:

——规定了要求的安全功能,以及相应的安全完整性等级(见 GB/T 20438.1—2017 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—2017 的 7.6);

——给每个 E/E/PE 系统中的软件分配功能(见 GB/T 20438.2—2017 的 7.2)。

b) 为所有分配给软件的安全功能确定软件架构(见 GB/T 20438.3—2017 的 7.4 及附录 A)。

c) 与 E/E/PE 安全相关系统的供应商/开发者一起复审软件和硬件架构,及软件和硬件之间进行折衷方案的安全影响(见 GB/T 20438.2—2017 的图 4)。当需要时应进行迭代。

d) 开始编制软件安全验证和确认计划(见 GB/T 20438.3—2017 的 7.3 和 7.9)。

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—2017 的 7.5),同时编制用户和维护人员在操作系统时所依据的软件方面规程(见 GB/T 20438.3—2017 的 7.6 和 A.2 k))。

g) 与硬件开发者一起(见 GB/T 20438.2—2017 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—2017 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/PE 安全相关系统软件进行修改,则应重新进行 GB/T 20438.3 的这个相应阶段(见 GB/T 20438.3—2017 的 7.8)。

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—2017 的 7.9)和功能安全评估(见 GB/T 20438.3—2017 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—2017 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—2017 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—2017 的附录 D)。

注 2:在应用上述步骤时如果在编制安全计划过程中建立合理性证明文档,那么 GB/T 20438 中规定的那些措施可以被替代(见 GB/T 20438.1—2017 的第 6 章)。

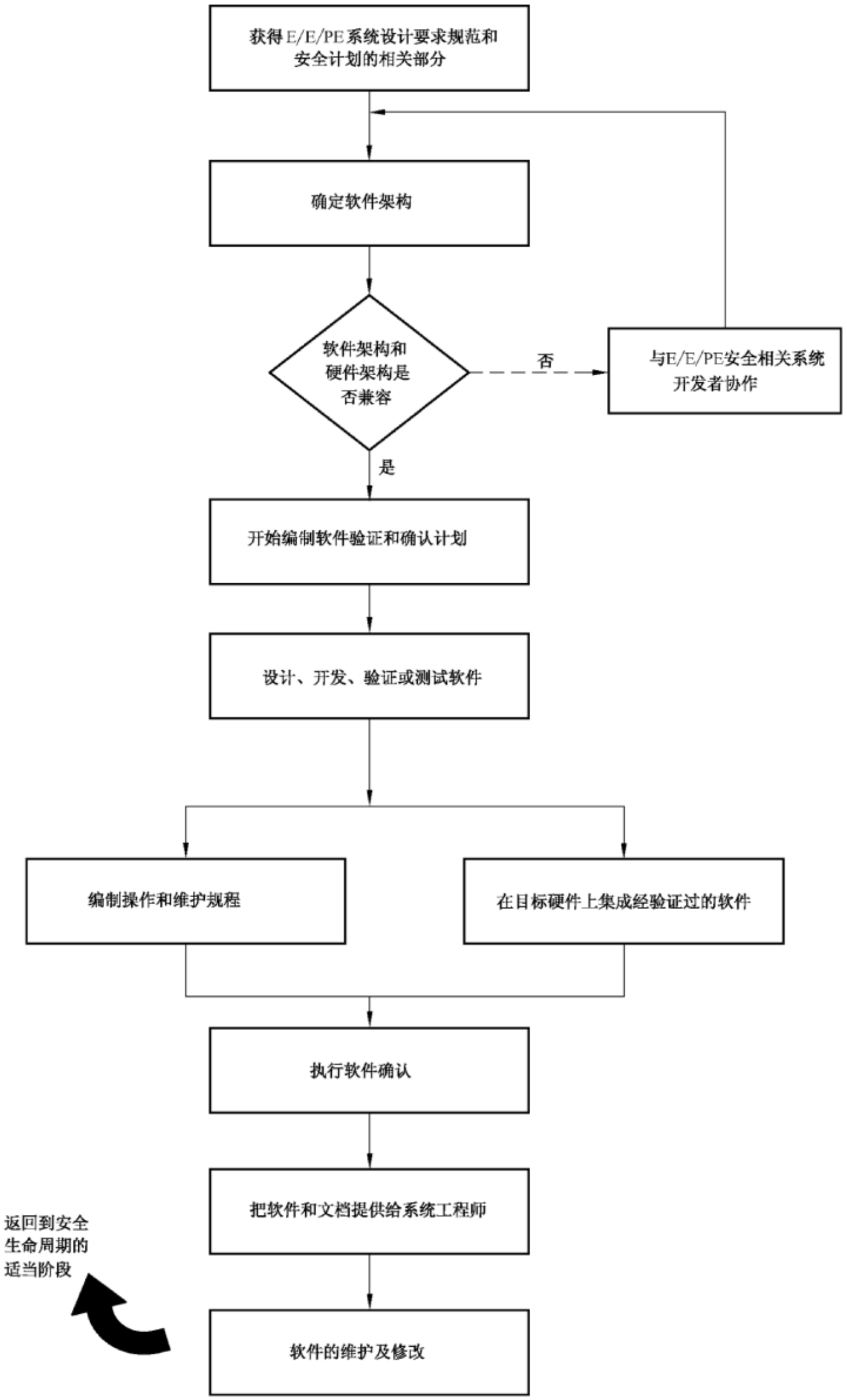


图 A.3　GB/T 20438.3 的应用

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计算的可行技术。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估技术。但它的确提供了一种简便的评估 E/E/PE 安全相关系统性能的方法，也提供了使用从传统的可靠性计算技术中获取的可替代技术的指导方法。

注 1：本部分中系统描述的架构仅是举例，并不详尽，还可能存在其他架构。

注 2：见参考文献[17]。

很多可靠性技术都可或多或少用来分析 E/E/PE 安全相关系统的硬件安全完整性，通常它们按照以下两种观点来分类：

——静态（布尔）和动态（状态/转移）模型；

——分析和蒙特卡洛（Monte Carlo）仿真计算。

布尔模型包括了描述基础部件失效与整个系统失效之间静态逻辑关系的所有模型。可靠性框图（RBD）（见 GB/T 20438.7—2017 中 C.6.4 和参考文献[4]）和故障树（FT）（见 GB/T 20438.7—2017 中 B.6.6.5 和 B.6.6.9 以及参考文献[18]）都属于布尔模型。

状态/迁移模型描述了系统对于事件（失效、维修、测试等）做出响应（状态之间的跳转）的所有模型。马尔可夫模型（见 GB/T 20438.7—2017 中 B.6.6.6 和参考文献[5]）、佩特里网（Petri nets）（见 GB/T 20438.7—2017 B.2.3.3 和 B.6.6.10 以及参考文献[19]）和形式语言模型都属于状态/迁移模型。讨论两种马尔可夫方法：一种是基于具体公式的简化方法（B.3）；一种是根据马尔可夫图直接计算的通用方法（B.5.2）。对于不适用马尔可夫模型的安全系统，可以用蒙特卡洛（Monte-Carlo）仿真代替。以当前的计算机水平，甚至能够达到 SIL 4 的计算要求。本附录 B.5.3 和 B.5.4 概要讲述了基于佩特里网（Petri nets）和形式语言模型的蒙特卡洛（Monte-Carlo）仿真方法（见 GB/T 20438.7—2017 的 B.6.6.8）。

上文提到的简化方法是基于 RBD 图形化说明、马尔可夫公式（由泰勒理论发展而来）以及略微保守的基础假设（见 B.3.1）共同建立的。

所有这些方法可用于大多数安全相关系统。对于特定应用决定采用何种特定技术时，使用者是否有能力使用该技术非常关键，这一点可能比实际使用的技术更加重要。分析人员有责任验证特定方法的基础假设条件是否得到满足，或者所做任意调整是否能够按要求获得足够且保守的结果。在可靠性数据较差或者共因失效占主导时，使用最简单的模型/技术就足够。精度损失的影响显著与否，取决于具体情况。

如果使用软件程序进行运算，使用者应理解软件中使用的公式/技术，以确保公式/技术的使用适合此特定应用。使用者也应通过检查一些手工计算测试用例的输出结果，对软件进行验证。

在 EUC 控制系统失效对 E/E/PE 安全相关系统提出要求，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因失效机制产生同时失效的可能性。存在这样的故障就会导致比预期更大的残余风险，除非已作适当的处理。

B.2 基本概率计算的注意事项

B.2.1 介绍

图 B.1 中的可靠性框图(RBD)表示了一个安全回路,安全回路由三个传感器(A,B,C),一个逻辑运算器(D),两个最终执行元件(E,F)以及共因失效(CCF)组成。

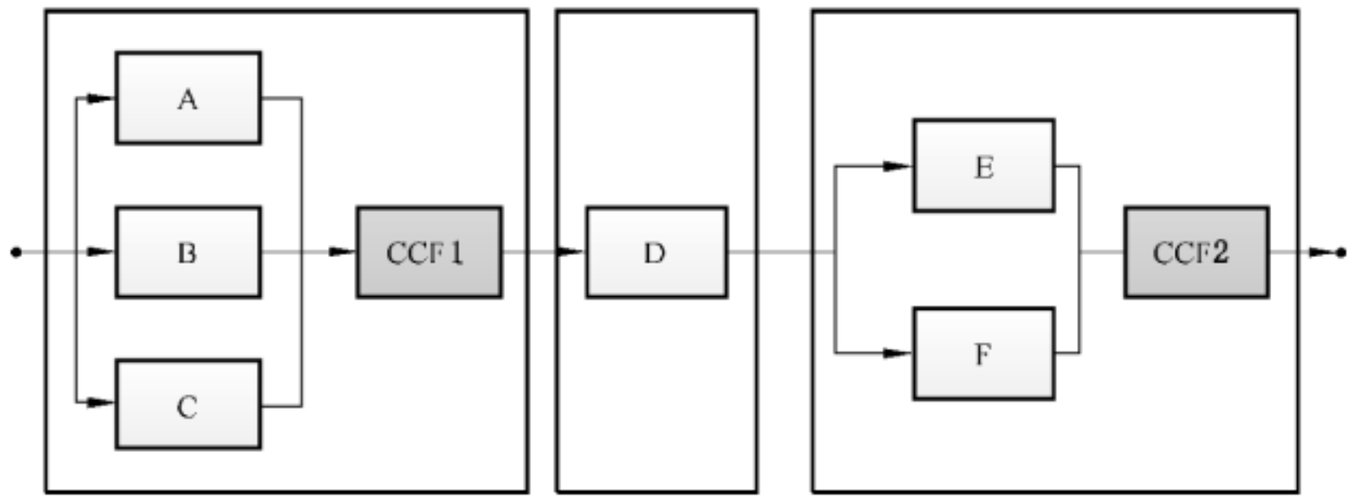


图 B.1 完整安全回路的可靠性框图

使用可靠性框图有利于确定导致 E/E/PE 安全相关系统失效的五部分失效组合,每一部分称为一个最小割集:

——(A,B,C)为三重失效;

——(E,F)为二重失效;

——(D)(CCF1)(CCF2)为单个失效。

B.2.2 低要求 E/E/PE 安全相关系统

当 E/E/PE 安全相关系统工作于低要求模式,标准要求评估系统的 PFD_{avg} 值(即系统的平均不可用值)。它是 $MDT(T)$ 与 T 的比值,其中 MDT 是 E/E/PE 安全相关系统在【0,T】时间内的平均不工作时间。

对于安全相关系统,其失效概率通常比较低,两个最小割集同时失效的概率可以忽略不计。因此,用每一割集平均不工作时间求和来保守估计整个系统的平均不工作时间。根据图 B.1,我们得到:

$$MDT \approx MDT^{ABC} + MDT^{D} + MDT^{EF}$$

MDT 除以 T:

$$PFD_{avg} \approx PFD_{avg}{}^{ABC} + PFD_{avg}{}^{D} + PFD_{avg}{}^{EF}$$

所以,对于串联部分,当数值远远小于 1 时,PFD_{avg} 的计算与常用概率计算非常类似。

然而对于并联部分,多重失效同时发生才会引起功能丧失,例如(E,F)。显然,MDT^{EF} 无法通过 MDT^{E} 和 MDT^{F} 来直接计算,(E,F)的 MDT 值需用如下方式计算:

$$MDT^{EF} = \int_0^T PFD^{E}(t) PFD^{E}(t)\,dt$$

因此,常用概率计算方法(加法和乘法)对于并联部分的 PFD_{avg} 计算(积分)不再有效。PFD_{avg} 不具有真实概率属性,它的真实概率同化性很可能会导致非保守的结果出现。尤其是,不可能仅仅通过传统方法将 E/E/PE 安全相关系统组件的 PFD_{avg},i 组合起来,从而得到 PFD_{avg} 值。因此使用商业布尔软件时,分析人员需要提高警惕,避免在安全方面出现不期望的非保守计算。

示例:对于一个(1oo2)冗余通道,未检测到的危险失效率 λ_{DU},检验测试时间间隔 τ,不正确的概率模型计算结果为 $(\lambda_{DU}.\tau)^2/4$,而正确结果为 $(\lambda_{DU}.\tau)^2/3$。

计算可以采用分析或者蒙特卡洛(Monte-Carlo)仿真方法。本附录描述了如何使用基于布尔模型(RBD 或 FT)或者状态/迁移模型[马尔可夫模型,佩特里网(Petri nets)等]的传统可靠性模型来进行计算。

B.2.3 连续或高要求模式 E/E/PE 安全相关系统

B.2.3.1 通用 *PFH* 公式

当 E/E/PE 安全相关系统工作在连续或高要求模式时,标准要求计算安全相关系统的 *PFH* 值(即其平均危险失效频率)。下面给出了绝对失效密度函数 $W(t)$(也称失效频率函数)在我们关注时间周期上的平均值。

$$PFH(T)=\frac{1}{T}\int_0^T W(t)\,\mathrm{d}t$$

当 E/E/PE 安全相关系统工作在连续模式,并且作为最终的安全保护层,那么整个安全相关系统的失效将直接导致进入潜在的危险状态。因此对于引起整个安全功能丧失的失效,在计算中无法对整个安全系统的修复做出考虑。如果其他安全保护层或者设备失效,虽然导致整个安全相关系统的故障,但不会直接导致潜在的危险,那么在风险降低计算中就可以对安全相关系统的诊断及修复做出考虑。

B.2.3.2 不可靠性情况(单一保护层工作于连续模式)

这种情况是与工作于连续模式的 E/E/PE 安全相关系统作为最终的安全保护层相关联的。因此一旦安全系统失效,就会有潜在危险发生。在我们关注的时间周期内整个系统的失效是不可接受的。

在这种情况下,在我们关注的时间周期内,使用不可靠性方法来计算 *PFH*:

$$F(T):PFH(T)=\frac{1-\exp\left[-\int_0^T \Lambda(t)\,\mathrm{d}t\right]}{T}=\frac{F(T)}{T}$$

整个系统的失效率 $\Lambda(t)$可能与时间有关也可能是常数。

当 $\Lambda(t)$与时间有关时, $PFH(T)=\dfrac{1-\exp(-\Lambda_{avg}\,T)}{T}\approx\Lambda_{avg}$

当系统由可完全并快速修复的元件组成,并且元件的失效率和修复率都为常数(例如:可检测危险失效)时,$\Lambda(t)$可以迅速达到一个近似常量值 Λ_{as},且 $PFH(T)<<1$,则有:

$$PFH(T)=\frac{1-\exp(-\Lambda_{as}\,T)}{T}\approx\Lambda_{as}=\frac{1}{MTTF}$$

仅当 E/E/PE 安全相关系统工作在连续模式,并且系统仅包含安全和可检测的危险失效时(即可快速检测和可修复),Λ_{as}存在。应考虑能够直接导致整个系统安全功能失效的不可修复失效。如果是一个考虑了检验测试的相关冗余配置系统,则不与近似失效率关联,需要使用前面的等式计算。分析人员需要确认哪种情况适用。

B.2.3.3 不可用性情况(多重保护层)

当工作于连续模式的 E/E/PE 安全相关系统不是最终的保护层,安全系统的失效只是增加了对其他安全层的要求频率,或者当系统工作于高要求模式,此时系统能够(自动或者手动)检测和修复故障,该故障可以直接引起在预期要求时间周期内的安全功能丧失。在这种情况下,整个系统的失效是可以修复的,从而就可以根据系统的可用性,即 $A(t)$以及条件失效密度函数 $\Lambda_v(t)$来计算 *PFH*。

另外,当系统构成元件有完全快速的修复能力(在任何降级情况下,有较高概率快速返回良好工作状态),$\Lambda_v(t)$可以很快达到它的近似值 Λ_{vas}。并且,Λ_{vas}也是对整个系统的真实近似失效率 Λ_{as}的一个

好的近似值，关于Λ_{as}的介绍见 B.2.3.2。

有如下近似：

$$PFH(T)=\frac{1}{MUT+MDT}=\frac{1}{MTBF}\approx\frac{1}{MUT}\approx\frac{1}{MTTF}$$

式中：

MUT ——平均工作时间；

MDT ——平均不工作时间；

$MTBF$ ——平均失效间隔时间；

$MTTF$ ——平均失效前时间。

B.2.3.4 关于失效率的考虑

上面提到的公式中使用整体系统失效率$\Lambda(t)$。对$\Lambda(t)$的评估不容易做到而且还有一些需要注意的地方。

串联结构非常简单，计算时直接把失效率相加就可以。在表 B.1 中，我们可以得到$\Lambda(t)=\Lambda^{abc}(t)+\lambda^{CCF1}(t)+\lambda^{d}(t)+\Lambda^{ef}(t)+\lambda^{CCF2}(t)$。其中$\Lambda(t)$是 E/E/PE 安全相关系统整体失效率，$\Lambda^{abc}(t)$、$\lambda^{CCF1}(t)$、$\lambda^{d}(t)$、$\Lambda^{ef}(t)$、$\lambda^{CCF2}(t)$对应系统的 5 个最小割集失效率。

并联结构就不是这么简单了，因为独立组件失效率之间都有或多或少的关系。例如，我们来分析(E,F)割集：

1) 在 E 和 F 不能做到立即恢复(例如不可检测的危险失效)时，$\Lambda^{ef}(t)$会在 0 到λ(E 或者 F 的失效率)连续变化。在两个组件之一发生失效时，$\Lambda^{ef}(t)$会达到一个近似值。当t远远大于$1/\lambda$时，$\Lambda^{ef}(t)$达到近似是一个非常缓慢的过程。如果 E 和 F 带有周期性的检验测试并且检验测试时间间隔$\tau<<1/\lambda$时，$\Lambda^{ef}(t)$的近似值在实际情况中将无法达到。

2) 当 E 和 F 可以在相对较短的时间周期内进行恢复(例如可检测的危险失效)时，$\Lambda^{ef}(t)$可以很快达到一个近似值$\Lambda_{as}^{ef}=2\lambda^{2}/u$，并且这个近似值可以做为等效常量失效率来用。当$t$大于两、三倍的组件$MTTR$值时，$\Lambda^{ef}(t)$达到近似值。这属于我们前面讨论过的可以完全快速修复系统的一种特殊情况。

因此，在通常状况下，评估整个系统的失效率意味着将进行比较复杂的计算，其复杂程度远远大于简单串联结构。

B.3 可靠性框图方法，假定常量失效率

B.3.1 基础假设

计算基于以下假设：

——在要求时系统出现失效的平均概率低于10^{-1}，或者系统危险失效频率小于10^{-5}/h；

注 1：这种假设是指 E/E/PE 安全相关系统在 GB/T 20438 系列标准范围之内且对应了 SIL1(见 GB/T 20438.1—2017 的表 2 和表 3)

——在系统寿命内元器件失效率为常量；

——传感器(输入)子系统包含实际的传感器、其他元器件、接线，但不包括信号通过表决或其他处理方式被首先进行组合的那些元器件(例如，对于双传感器通道，其配置如图 B.2 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(输出)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，还包括最终执行元器件；

——作为计算输入和表格中的硬件失效率是子系统的单通道失效率(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);

——在一个表决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—2017 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。

——每个安全功能都能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)。不理想的检验测试的影响,可以查询 B.3.2.5;

——检验测试的间隔至少要比平均修理时间(*MRT*)大一个数量级;

——对于每个子系统都有自身的检验测试间隔以及平均修理时间(*MRT*);

——预计的要求间隔至少比检验测试时间间隔大一个数量级;

——对于所有在低要求运行模式下运行的子系统以及在高要求或连续运行模式下工作的 1oo2、1oo2D、1oo3、2oo3 表决组,诊断覆盖率规定的失效部分,在平均恢复时间内被检测和修复,平均恢复时间决定硬件安全完整性的需求。

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

注 3:对 1oo2、1oo2D、1oo3、2oo3 表决组,假设任何修理均在线进行。配置一个 E/E/PE 安全相关系统在检测到任何故障时使 EUC 进入一种安全状态,可以改善要求时的平均失效概率,改善程度取决于诊断覆盖率。

——对于在高要求或连续运行模式下工作的 1oo1、2oo2 表决组,E/E/PE 安全相关系统在检测到危险故障后即进入安全状态。为此,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 4:过程安全时间已在 GB/T 20438.4—2017 的 3.6.20 中定义

——当电源失效不能对断电跳闸型(失电安全型)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(得电安全型),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“通道”这个术语时,它只限于所讨论的那部分系统,通常指传感器子系统、逻辑子系统或最终元件子系统;

——缩略的术语在表 B.1 中有所描述。

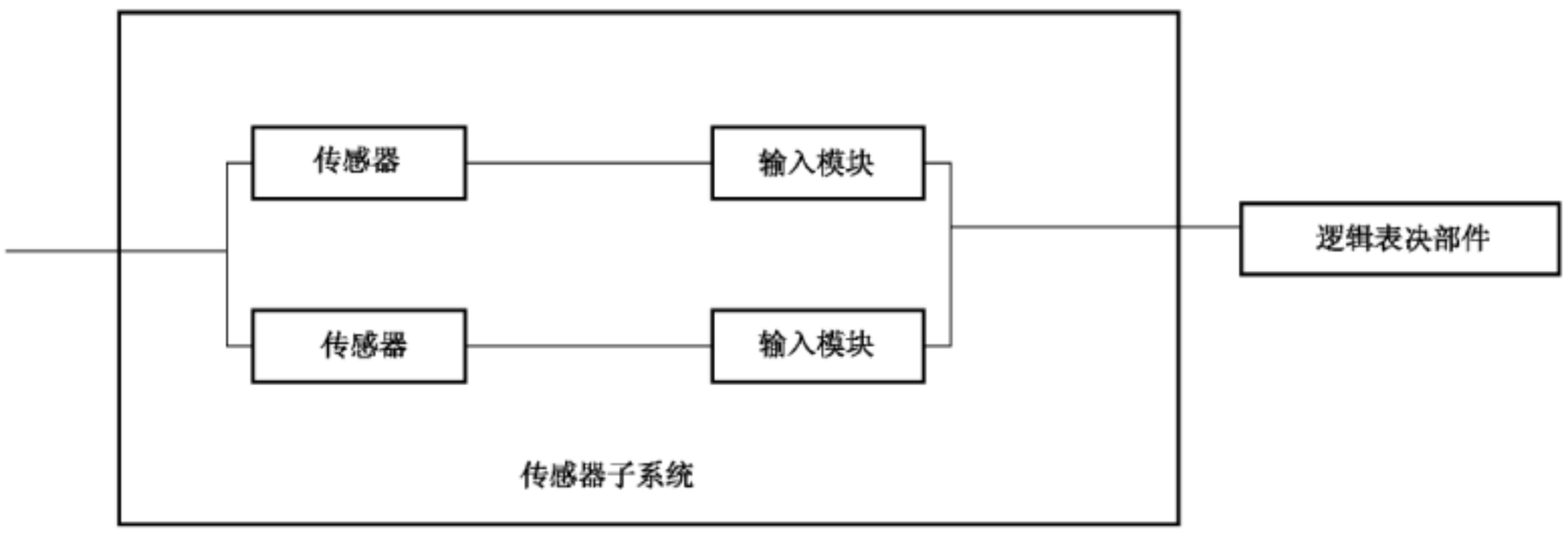


图 B.2　两个传感器通道配置示例

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

缩略语	术语(单位)	表 B.2～表 B.5 及表 B.10～表 B.13 的参数范围
T_1	检验测试时间间隔(h)	一个月(730 h)[1] 三个月(2 190 h)[1] 六个月(4 380 h) 一年(8 760 h) 两年(17 520 h)[2] 十年(87 600 h)[2]
MTTR	平均恢复时间(h)	8 h 注：$MTTR=MRT=8$ h 基于如下假设：采用自动诊断，诊断到危险失效的时间<<*MRT*
MRT	平均修理时间(h)	8 h 注：$MTTR=MRT=8$ h 基于如下假设：采用自动诊断，诊断到危险失效的时间<<*MRT*
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份比表示)(表 B.2～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 B.10～表 B.13 中假设 $\beta=2\times\beta_D$)	1% 5% 10%
λ_{DU}	子系统中一个通道的未检测到的危险失效率(每小时)	0.05×10^{-6} 0.25×10^{-6} 0.5×10^{-6} 2.5×10^{-6} 5×10^{-6} 25×10^{-6}
PFD_G	表决通道组在要求时的平均失效概率(如果传感器子系统、逻辑子系统或最终元件子系统分别对应一个表决组，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在要求时的平均失效概率	
PFH_G	表决通道组的平均危险失效频率(如果传感器、逻辑或最终元件子系统分别对应一个表决组，则 PFH_G 分别等于 PFH_S、PFH_L 或 PFH_{FE})	

表 B.1（续）

缩略语	术语(单位)	表 B.2～表 B.5 及表 B.10～表 B.13 的参数范围
PFH_S	传感器子系统的平均危险失效频率	
PFH_L	逻辑子系统的平均危险失效频率	
PFH_{FE}	最终元件子系统的平均危险失效频率	
PFH_{SYS}	E/E/PE 安全相关系统中一个安全功能的平均危险失效频率	
λ	子系统中一个通道的总失效率(每小时)	
λ_D	子系统中一个通道的危险失效率(每小时),等于 0.5λ(假设 50%的危险失效和 50%的安全失效)	
λ_{DD}	子系统中一个通道被检测到的危险失效率(每小时)(它是子系统中该通道所有被检测到的危险失效率的总和)	
λ_{DU}	子系统中一个通道未检测到的危险失效率(每小时)(它是子系统中该通道所有未检测到的危险失效率的总和)	
λ_{SD}	子系统中一个通道被检测到的安全失效率(每小时)(它是子系统中该通道所有被检测到的安全失效率的总和)	
t_{CE}	1oo1、1oo2、2oo2、2oo3 结构中通道的等效平均不工作时间(h)(它是子系统通道中所有部件的组合不工作时间)	
t_{GE}	1oo2、2oo3 结构中表决组的等效平均不工作时间(h)(它是表决组中所有通道的组合不工作时间)	
t'_{CE}	1oo2D 结构中通道的等效平均不工作时间(h)(它是子系统通道中所有部件的组合不工作时间)	
t'_{GE}	1oo2D 结构中表决组的等效平均不工作时间(h)(它是表决组中所有通道的组合不工作时间)	
T_2	要求之间的时间间隔(h)	
K	1oo2D 系统中自测试电路的成功百分比	
PTC	检验测试覆盖率	
[1] 仅对于高要求或连续运行模式。 [2] 仅对于低要求运行模式。		

B.3.2 要求时的平均失效概率(对于低要求运行模式)

B.3.2.1 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,是通过计算和组合执行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.3):

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

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 ——为传感器子系统要求时的平均失效概率;

PFD_L ——为逻辑子系统要求时的平均失效概率;

PFD_{FE} ——为最终元件子系统要求时的平均失效概率。

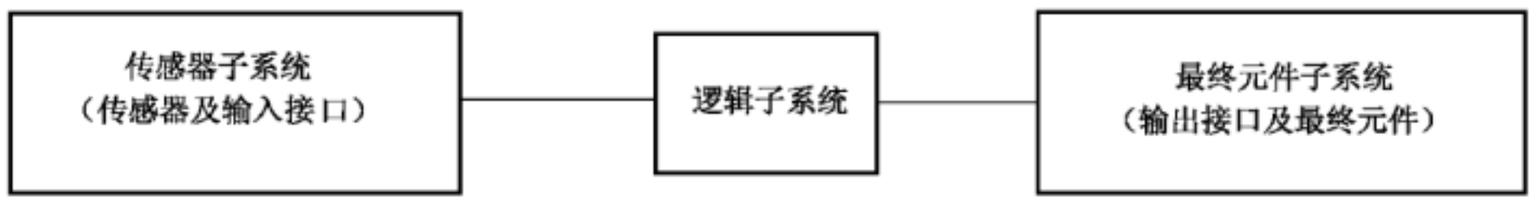


图 B.3　子系统结构

为了确定每一个子系统在要求时的平均失效概率，在子系统中应依次遵循下列步骤：

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)各部件的框图。例如，传感器子系统的部件可能是传感器、安全栅、输入调理电路；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理电路，安全栅及执行器。将每一个子系统描绘成 1oo1、1oo2、2oo2、1oo2D、1oo3、2oo3 表决组。

b)　参考相关的表 B.2～表 B.5，它们分别提供了六个月、一年、两年以及十年检验测试时间间隔的数据。这些表也假定了，一旦发现失效，则每次失效的平均恢复时间为 8 h。

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

——架构(例如 2oo3)；

——每个通道的诊断覆盖率(例如 60%)；

——每个通道的危险失效率(每小时)λ_D，(例如，2.5×10^{-6})；

——表决组中通道之间相互作用的共因失效的 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(见表 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 $PFDs$ 或 PFD_{FE} 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；

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

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

这个公式用于所有 PFD 和系统失效率的计算等式中，它也是元器件失效率和元器件平均不工作时间的一个函数。当系统包含一定数量的组件，并且要计算组合组件的整体 PFD 或者系统失效率时，那么在等式中通常需使用一个唯一的 MDT 值。然而有不同的失效检测机理的每个组件可能具有不同 MDT 值，有相同失效机理的不同组件也有可能具有不同 MDT 值，在这种情况下，有必要计算一个可以代表所有组件的唯一 MDT 值。这个计算需要考虑到所有路径的整体失效率，然后根据单个路径的失效率所占整体失效率的权重，将每个路径的 MDT 值按比例进行等价计算。

如果有两个组件串联连接，其中一个检验测试时间间隔为 T_1，另外一个为 T_2，那么这个等效的唯一 MDT 值计算如下：

$$\lambda_T=\lambda_1+\lambda_2$$

和

$$MDT_E=\frac{\lambda_1}{\lambda_T}\left(\frac{T_1}{2}\right)+\frac{\lambda_2}{\lambda_T}\left(\frac{T_2}{2}\right)$$

B.3.2.2　低要求运行模式的架构

注 1：按顺序阅读本条，因为对几种架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 B.3.1 的假设而得出的。

注 3：下面的例子是典型配置，并不详尽。

B.3.2.2.1 1oo1

这种架构包括一个单通道，在这种架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。

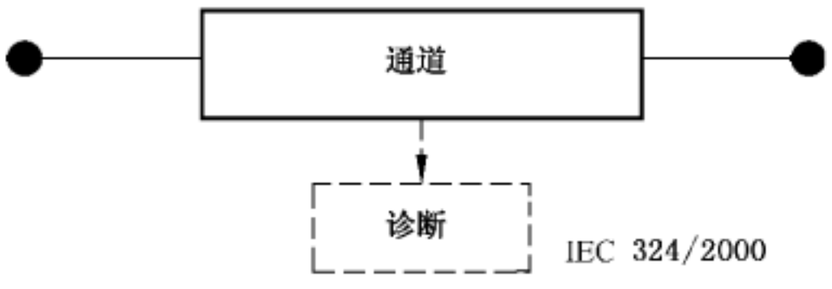


图 B.4 1oo1 物理框图

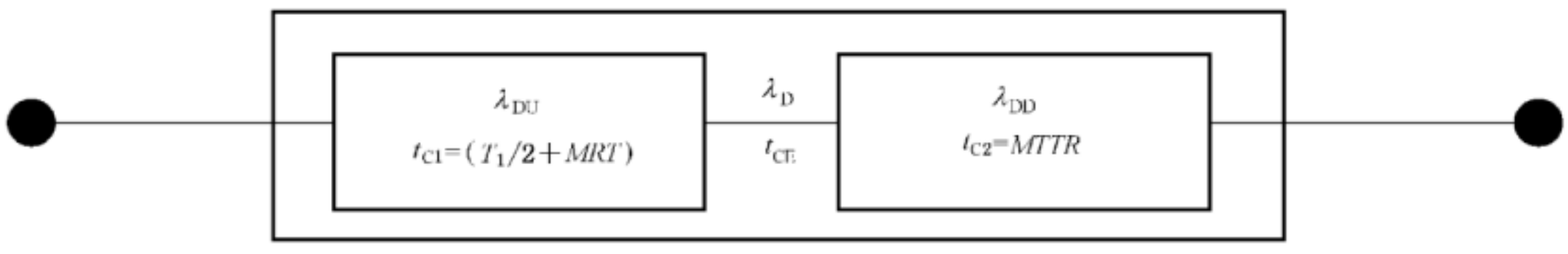


图 B.5 1oo1 可靠性框图

图 B.4 与图 B.5 包括了有关的框图，通道的危险失效率为：

$$\lambda_D = \lambda_{DU} + \lambda_{DD}$$

图 B.5 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}，通道的等效平均不工作时间 t_{CE}，等于两部分各自的不工作时间 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：

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

对于每种架构，已被检测和未被检测到的危险失效率如下：

$$\lambda_{DU} = \lambda_D(1 - DC)；\lambda_{DD} = \lambda_D DC$$

对于一个具有由危险失效而导致不工作时间为 t_{CE} 的通道：

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

$$\approx \lambda_D t_{CE} \quad \text{因为 } \lambda_D t_{CE} << 1$$

因此，对于 1oo1 架构，在要求时的平均失效概率为：

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

B.3.2.2.2 1oo2

此架构由两个并联的通道构成，每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。

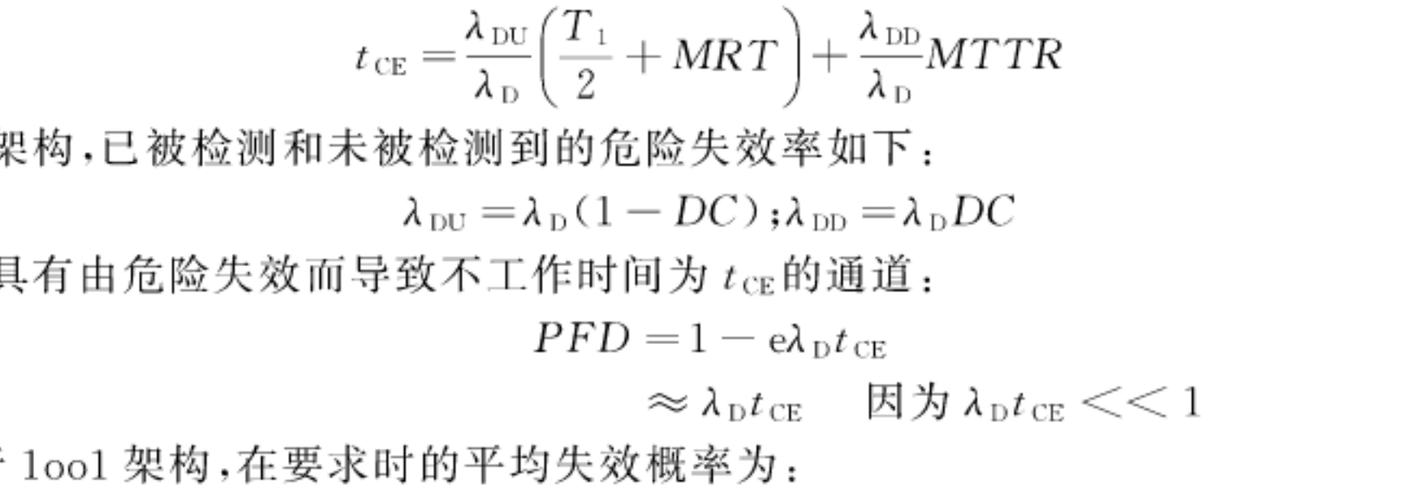


图 B.6 1oo2 物理框图

图 B.6 与图 B.7 中包含了相关的框图，t_{CE}的值在 B.3.2.2.1 中已经给出，但是现在还需计算系统等效不工作时间 t_{GE}，表示如下：

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

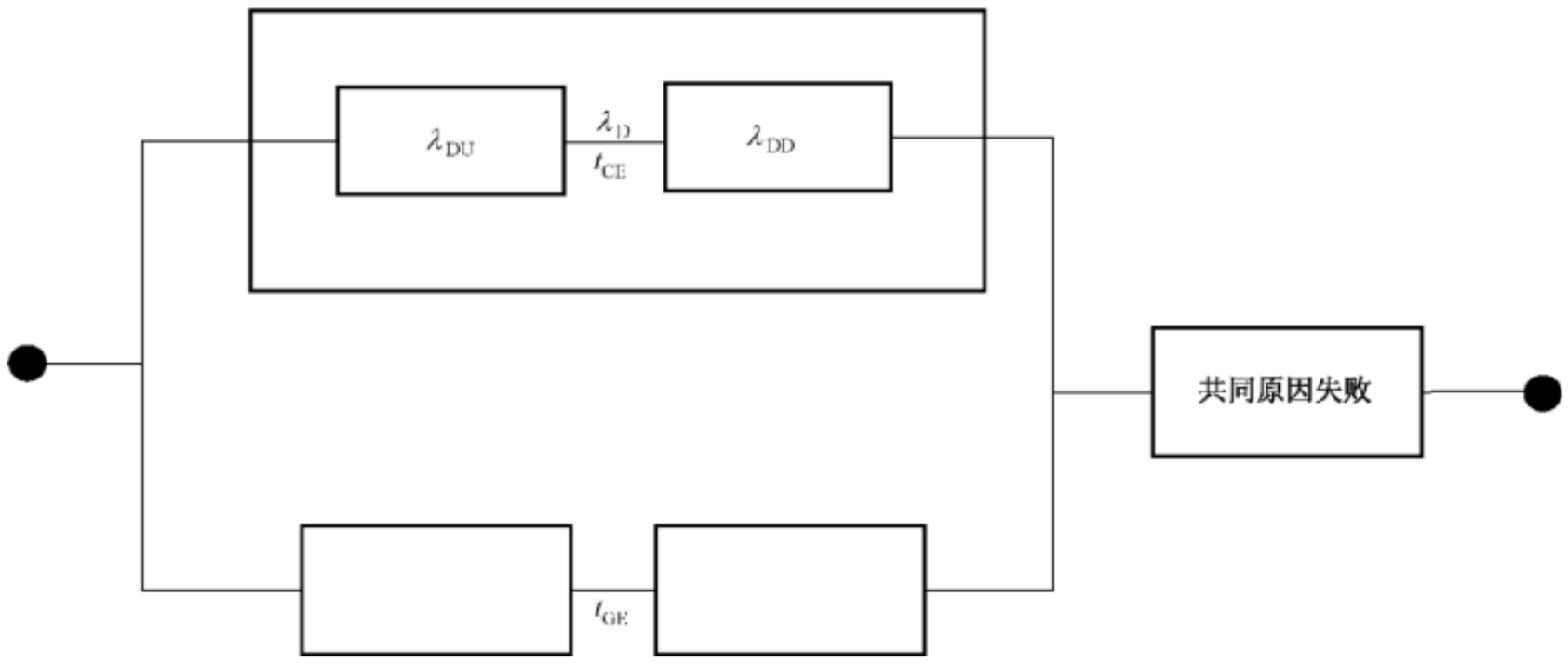


图 B.7　1oo2 可靠性框图

此架构的要求时平均失效概率为：

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

B.3.2.2.3　2oo2

此架构由并联的两个通道构成，因此，两个通道都要求安全功能时，动作才发生。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。

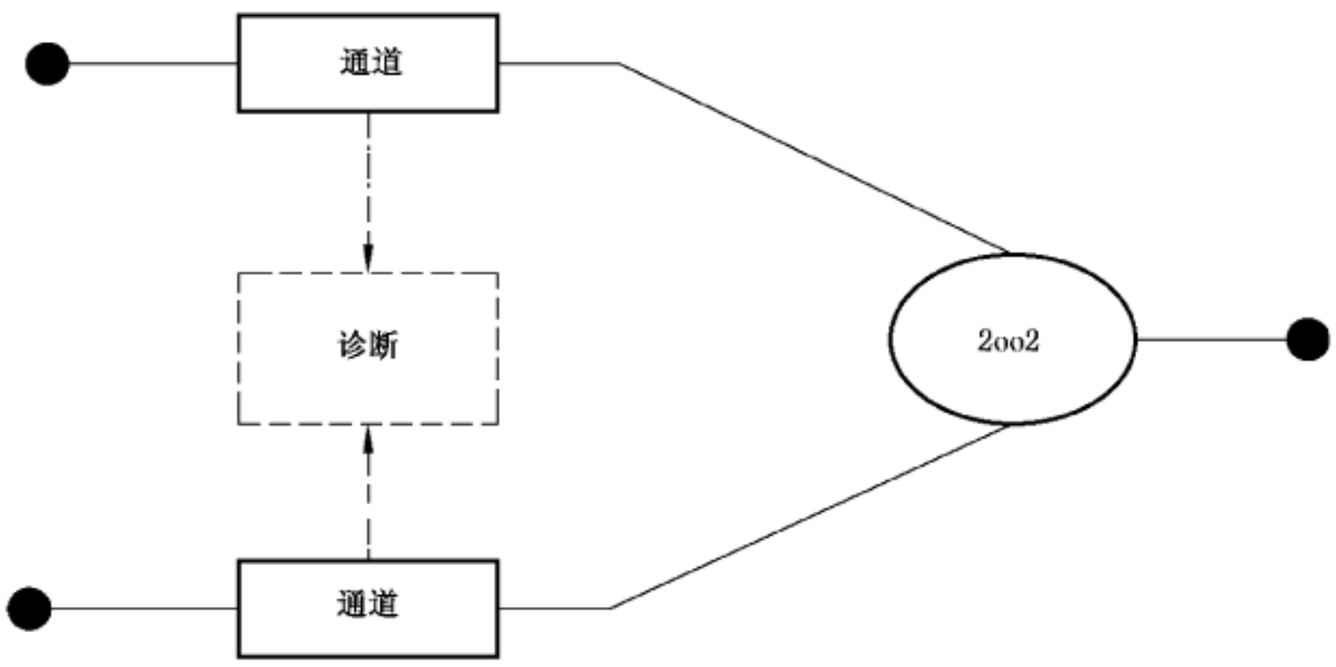


图 B.8　2oo2 物理框图

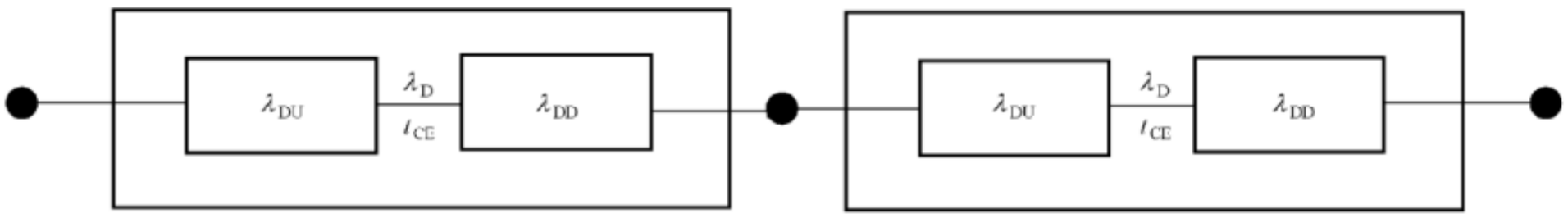


图 B.9　2oo2 可靠性框图

图 B.8 与图 B.9 包含了相关的框图，t_{CE}的值已在 B.3.2.2.1 中给出，此架构在要求时的平均失效概

率如下：

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

B.3.2.2.4 1oo2D

此架构中由并联的两个通道构成，正常工作期间，两个通道都要求安全功能时，动作才发生。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，无论哪个通道都可通过独立的诊断方法确定另一通道的状态。通道的比较/切换机制不是100%的有效，因此要用 K 值来描述内部通道的比较/切换机制效率，也就是说，即使检测出一个通道有故障，输出依然可能保留2oo2表决形式。

注：参数 K 需要由FMEA来确定。

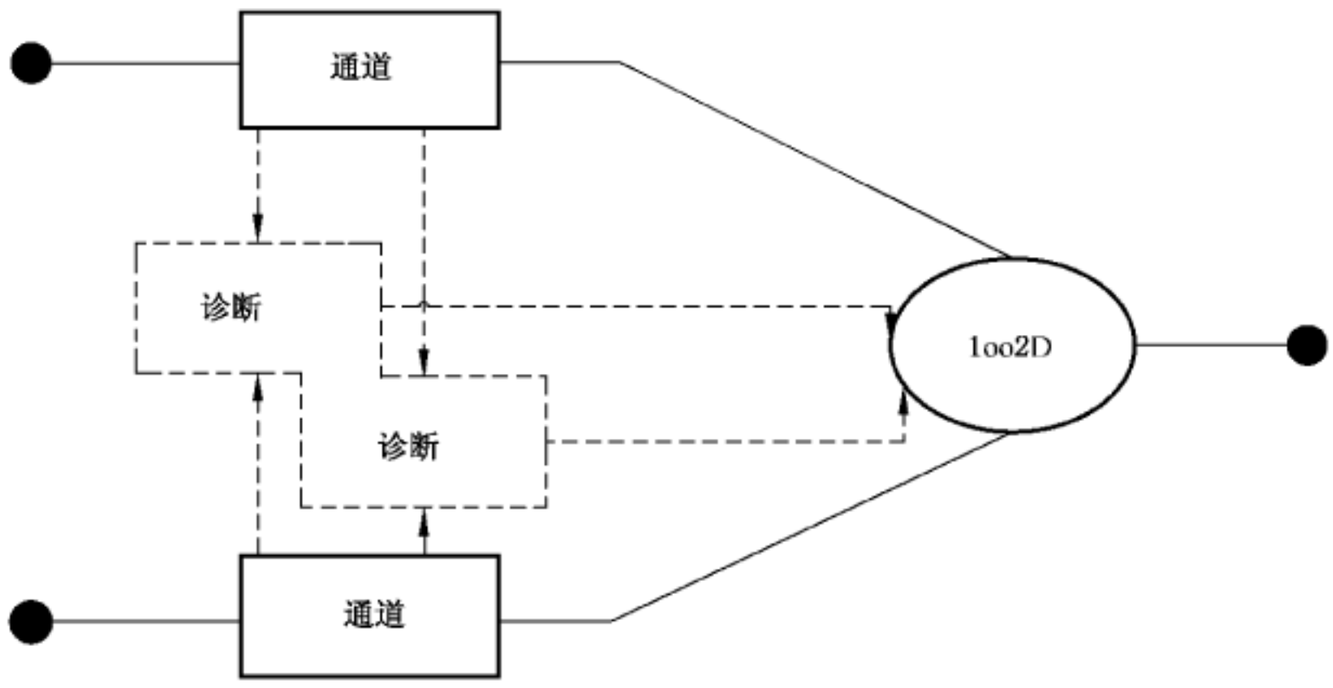


图 B.10 1oo2D 物理块图

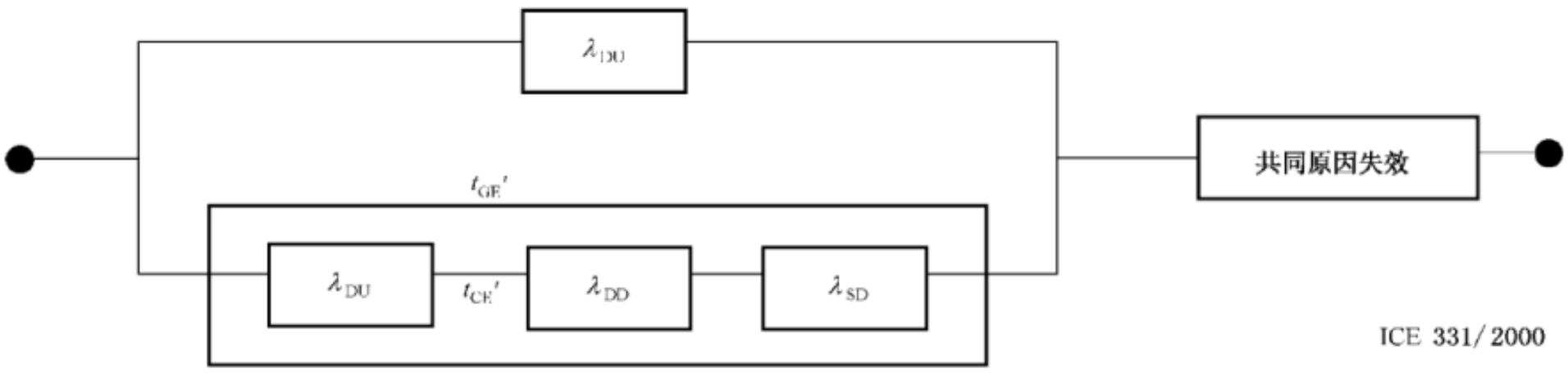


图 B.11 1oo2D 可靠性框图

每个通道中被检测的安全失效率如下：

$$\lambda_{SD} = \lambda_S DC$$

图B.10与图B.11包含相关的框图，B.3.2.2中的等效平均不工作时间的值与其他架构给出的数值不同，因此它们被表示为 t_{CE}' 与 t_{GE}'，它们的表达式如下：

$$t_{CE}' = [\lambda_{DU}/(T_1/2+MRT)+(\lambda_{DD}+\lambda_{SD})MTTR]/(\lambda_{DU}+\lambda_{DD}+\lambda_{SD})$$

$$t_{GE}' = T_1/3+MRT$$

架构在要求时的平均失效概率如下：

$$PFD_G = 2\ (1-\beta)\ \lambda_{DU}(\ (1-\beta)\ \lambda_{DU}+(1-\beta_D)\ \lambda_{DD}+\lambda_{SD})t_{CE}'t_{GE}' +$$
$$2(1-K)\lambda_{DD}t_{CE}' +\beta\lambda_{DU}(T_1/2+MRT)$$

B.3.2.2.5 2oo3

此架构由三个并联通道构成，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。

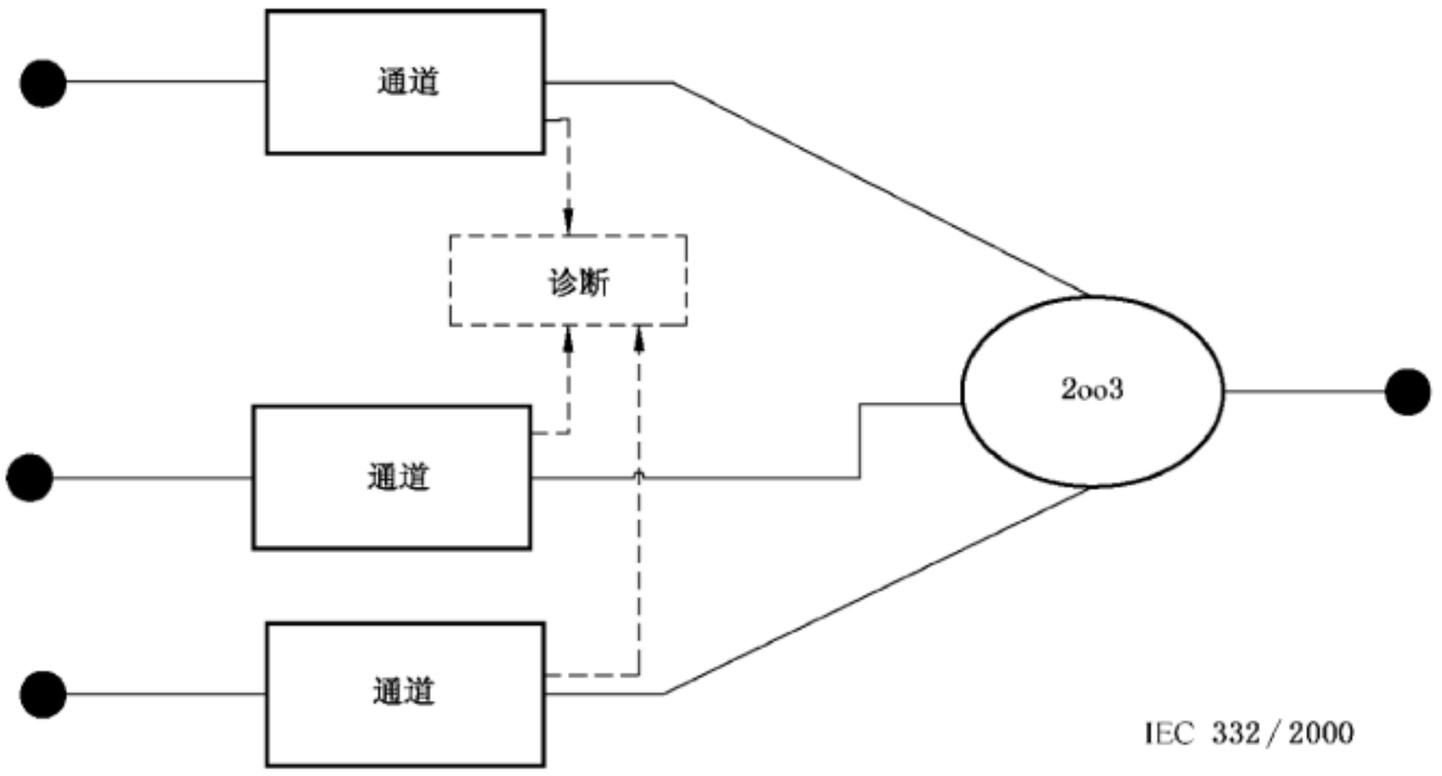


图 B.12　2oo3 物理框图

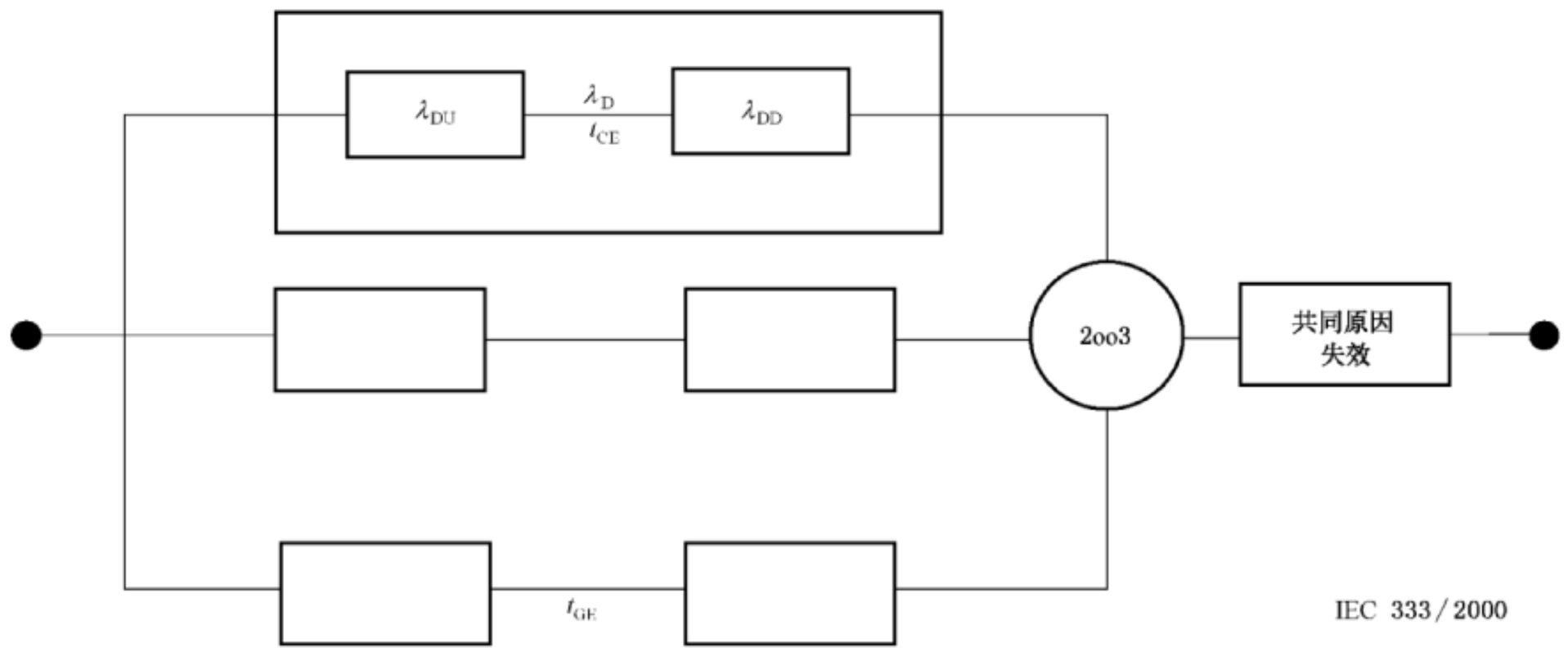


图 B.13　2oo3 可靠性框图

图 B.12 与图 B.13 包含了相关的框图。t_{CE}的值同 B.3.2.2.1 中给出的值相同，t_{GE}的值同 B.3.2.2.2 中给出的值相同。此架构在要求时的平均失效概率为：

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

B.3.2.2.6　1oo3

此架构由三个并联通道构成，其输出信号具有 1oo3 表决安排。

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。

可靠性框图与 2oo3 结构相同，但具有 1oo3 表决。t_{CE}的值同 B.3.2.2.1 中给出的值相同，t_{GE}的值同 B.3.2.2.2 中给出的值相同。此架构在要求时的平均失效概率为：

$$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^3 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}(T_1/2 + MRT)$$

其中

$$t_{G2E} = \lambda_{DU}/\lambda_D(T_1/4 + MRT) + \lambda_{DD}/\lambda_D MTTR$$

B.3.2.3 低要求运行模式的详表

表 B.2 检验测试时间间隔为 6 个月,平均恢复时间为 8 h 时,要求时的平均失效概率

结构	DC	λ_D=0.5E-07			λ_D=2.5E-07			λ_D=0.5E-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 (见注 3)	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%	1.4E-06	4.9E-06	9.3E-06	7.1E-06	2.5E-05	4.7E-05	1.4E-05	5.0E-05	9.3E-05
	90%	4.3E-07	1.3E-06	2.4E-06	2.2E-06	6.6E-06	1.2E-05	4.3E-06	1.3E-05	2.4E-05
	99%	6.0E-08	1.5E-07	2.6E-07	3.0E-07	7.4E-07	1.3E-06	6.0E-07	1.5E-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
1oo3	0%	2.2E-06	1.1E-05	2.2E-05	1.1E-05	5.5E-05	1.1E-04	2.2E-05	1.1E-04	2.2E-04
	60%	8.8E-07	4.4E-06	8.8E-06	4.4E-06	2.2E-05	4.4E-05	8.8E-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

表 B.2（续）

结构	DC	λ_D=2.5E-06			λ_D=0.5E-05			λ_D=2.5E-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			> 1E-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 （见注 3）	0%	1.5E-04	5.8E-04	1.1E-03	3.8E-04	1.2E-03	2.3E-03	5.0E-03	9.0E-03	1.4E-02
	60%	7.7E-05	2.5E-04	4.7E-04	1.7E-04	5.2E-04	9.5E-04	1.3E-03	3.0E-03	5.1E-03
	90%	2.2E-05	6.6E-05	1.2E-04	4.5E-05	1.3E-04	2.4E-04	2.6E-04	6.9E-04	1.2E-03
	99%	3.0E-06	7.4E-06	1.3E-05	6.0E-06	1.5E-05	2.6E-05	3.0E-05	7.4E-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
1oo3	0%	1.1E-04	5.5E-04	1.1E-03	2.2E-04	1.1E-03	2.2E-03	1.4E-03	5.7E-03	1.1E-02
	60%	4.4E-05	2.2E-04	4.4E-04	8.8E-05	4.4E-04	8.8E-04	4.6E-04	2.2E-03	4.4E-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

注 1：此表给出了 PFD_G 的示例值，它是根据 B.3.1 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、逻辑或最终元件子系统分别对应一个表决组，则 PFH_G 分别等于 PFH_S、PFH_L 或 PFH_{FE}（见 B.3.2.1）。

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。

注 3：假设安全失效率等于危险失效率并且 $K=0.98$。

表 B.3　检验测试时间间隔为 1 年，平均恢复时间为 8 h 时，要求时的平均失效概率

结构	DC	λ_D=0.5E-07			λ_D=2.5E-07			λ_D=0.5E-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		
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 （见注 3）	0%	4.5E-06	2.2E-05	4.4E-05	2.4E-05	1.1E-04	2.2E-04	5.0E-05	2.2E-04	4.4E-04
	60%	2.8E-06	9.8E-06	1.9E-05	1.4E-05	4.9E-05	9.3E-05	2.9E-05	9.9 E-05	1.9E-04
	90%	8.5E-07	2.6E-06	4.8E-06	4.3E-06	1.3E-05	2.4E-05	8.5E-06	2.6E-05	4.8E-05
	99%	1.0E-07	2.8E-07	5.0E-07	5.2E-07	1.4E-06	2.5E-06	1.0E-06	2.8E-06	5.0E-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
1oo3	0%	4.4E-06	2.2E-05	4.4E-05	2.2E-05	1.1E-04	2.2E-04	4.4E-05	2.2E-04	4.4E-04
	60%	1.8E-06	8.8E-06	1.8E-05	8.8E-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

表 B.3（续）

结构	DC	λ_D=2.5E-06			λ_D=0.5E-05			λ_D=2.5E-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			> 1E-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			> 1E-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		
1oo2D （见注 3）	0%	3.8E-04	1.2E-03	2.3E-03	1.1E-03	2.7E-03	4.9E-03	1.8E-02	2.5E-02	3.4E-02
	60%	1.7E-04	5.1E-04	9.5E-04	3.8E-04	1.1E-03	1.9E-03	3.9E-03	7.1E-03	1.1E-02
	90%	4.4E-05	1.3E-04	2.4E-04	9.1E-05	2.7E-04	4.8E-04	5.8E-04	1.4E-03	2.5E-03
	99%	5.2E-06	1.4E-05	2.5E-05	1.0E-05	2.8E-05	5.0E-05	5.4E-05	1.4E-04	2.5E-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
1oo3	0%	2.2E-04	1.1E-03	2.2E-03	4.6E-04	2.2E-03	4.4E-03	4.7E-03	1.3E-02	2.3E-02
	60%	8.8E-05	4.4E-04	8.8E-04	1.8E-04	8.8E-03	1.8E-03	1.0E-03	4.5E-03	8.9E-03
	90%	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
	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

注 1：此表给出了 PFD_G 的示例值，它是根据 B.3.1 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、逻辑或最终元件子系统分别对应一个表决组，则 PFH_G 分别等于 PFH_S、PFH_L 或 PFH_{FE}（见 B.3.2.1）。

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。

注 3：假设安全失效率等于危险失效率并且 $K=0.98$。

表 B.4　检验测试时间间隔为 2 年，平均恢复时间为 8 h 时，要求时的平均失效概率

结构	DC	λ_D=0.5E-07			λ_D=2.5E-07			λ_D=0.5E-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 （见注 3）	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	9.0E-04
	60%	5.7E-06	2.0E-05	3.7E-05	2.9E-05	9.9E-05	1.9E-04	6.0E-05	2.0E-04	3.7E-04
	90%	1.7E-06	5.2E-06	9.6E-06	8.5E-06	2.6E-05	4.8E-05	1.7E-05	5.2E-05	9.6E-05
	99%	1.9E-07	5.4E-07	9.8E-07	9.5E-07	2.7E-06	4.9E-06	1.9E-06	5.4E-06	9.8E-06
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
1oo3	0%	8.8E-06	4.4E-05	8.8E-05	4.4E-05	2.2E-04	4.4E-04	8.8E-05	4.4E-04	8.8E-04
	60%	3.5E-06	1.8E-05	3.5E-05	1.8E-05	8.8E-05	1.8E-04	3.5E-05	1.8E-04	3.5E-04
	90%	8.8E-07	4.4E-06	8.8E-06	4.4E-06	2.2E-05	4.4E-05	8.8E-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_D=2.5E-06			λ_D=0.5E-05			λ_D=2.5E-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			> 1E-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			> 1E-01		
	60%	1.8E-02			3.5E-02			> 1E-01		
	90%	4.4E-03			8.8E-03			4.4E-02		
	99%	4.8E-04			9.6E-04			4.8E-03		
1oo2D （见注 3）	0%	1.1E-03	2.7E-03	4.8E-03	3.4E-03	6.6E-03	1.1E-02	6.7E-02	7.7E-02	9.0E-02
	60%	3.8E-04	1.1E-03	1.9E-03	9.6E-04	2.3E-03	4.0E-03	1.3E-02	1.9E-02	2.6E-02
	90%	9.0E-05	2.6E-04	4.8E-04	1.9E-04	5.4E-04	9.8E-04	1.5E-03	3.2E-03	5.3E-03
	99%	9.6E-06	2.7E-05	4.9E-05	1.9E-05	5.4E-05	9.8E-05	1.0E-04	2.8E-04	5.0E-04
2oo3	0%	2.3E-03	3.7E-03	5.6E-03	8.3E-03	1.1E-02	1.4E-02	1.9E-01	1.8E-01	1.7E-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
1oo3	0%	4.6E-04	2.2E-03	4.4E-03	1.0E-03	4.5E-03	8.9E-03	2.4E-02	3.7E-02	5.5E-02
	60%	1.8E-04	8.8E-04	1.8E-03	3.6E-04	1.8E-03	3.5E-03	3.1E-03	9.9E-03	1.8E-02
	90%	4.4E-05	2.2E-04	4.4E-04	8.8E-05	4.4E-04	8.8E-04	4.6E-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

注 1：此表给出了 PFD_G 的示例值，它是根据 B.3.1 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、逻辑或最终元件子系统分别对应一个表决组，则 PFH_G 分别等于 PFH_S、PFH_L 或 PFH_{FE}（见 B.3.2.1）。

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。

注 3：假设安全失效率等于危险失效率并且 $K=0.98$。

表 B.5　检验测试时间间隔为 10 年，平均恢复时间为 8 h 时，要求时的平均失效概率

结构	DC	λ_D=0.5E-07			λ_D=2.5E-07			λ_D=0.5E-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-2		
	90%	4.4E-04			2.2E-03			4.4E-03		
	99%	4.5E-05			2.2E-04			4.5E-04		
1oo2D （见注 3）	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%	2.9E-05	9.9E-05	1.9E-04	1.7E-04	5.1E-04	9.5E-04	3.8E-04	1.1E-03	1.9E-03
	90%	8.4E-06	2.6E-05	4.8E-05	4.3E-05	1.3E-04	2.4E-04	9.0E-05	2.6E-04	4.8E-04
	99%	8.9E-07	2.6E-06	4.8E-06	4.5E-06	1.3E-05	2.4E-05	8.9E-06	2.6E-05	4.8E-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
1oo3	0%	4.4E-05	2.2E-04	4.4E-04	2.2E-04	1.1E-03	2.2E-03	4.6E-04	2.2E-03	4.4E-03
	60%	1.8E-05	8.8E-05	1.8E-04	8.8E-05	4.4E-04	8.8E-04	1.8E-04	8.8E-04	1.8E-03
	90%	4.4E-06	2.2E-05	4.4E-05	2.2E-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

表 B.5（续）

结构	DC	λ_D=2.5E-06			λ_D=0.5E-05			λ_D=2.5E-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%	> 1E-01			> 1E-01			> 1E-01		
	60%	4.4E-02			8.8E-02			> 1E-01		
	90%	1.1E-02			2.2E-02			> 1E-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	> 1E-01	> 1E-01	> 1E-01
	60%	3.4E-03	6.6E-03	1.1E-02	1.2E-02	1.8E-02	2.5E-02	> 1E-01	> 1E-01	> 1E-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%	> 1E-01			> 1E-01			> 1E-01		
	60%	8.8E-02			> 1E-01			> 1E-01		
	90%	2.2E-02			4.4E-02			> 1E-01		
	99%	2.2E-03			4.5E-03			2.2E-02		
1oo2D （见注 3）	0%	1.8E-02	2.5E-02	3.3E-02	6.6E-02	7.7E-02	9.0E-02	1.6E+00	1.5E+00	1.4E+00
	60%	3.9E-03	7.1E-03	1.1E-02	1.3E-02	1.9E-02	2.6E-02	2.6E-01	2.7E-01	2.8E-01
	90%	5.7E-04	1.4E-03	2.5E-03	1.5E-03	3.1E-03	5.2E-03	2.0E-02	2.7E-02	3.5E-02
	99%	4.6E-05	1.3E-04	2.4E-04	9.5E-05	2.7E-04	4.9E-04	6.0E-04	1.5E-03	2.5E-03
2oo3	0%	4.8E-02	5.0E-02	5.3E-02	1.9E-01	1.8E-01	1.7E-01	4.6E+00	4.0E+00	3.3E+00
	60%	8.3E-03	1.1E-02	1.4E-02	3.2E-02	3.5E-02	4.0E-02	7.6E-01	7.1E-01	6.6E-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
1oo3	0%	4.7E-03	1.3E-02	2.3E-02	2.4E-02	3.7E-02	5.5E-02	2.5E+00	2.0E+00	1.6E+00
	60%	1.0E-03	4.5E-03	8.9E-03	3.0E-03	9.8E-03	1.8E-02	1.7E-01	1.8E-01	1.9E-01
	90%	2.2E-04	1.1E-03	2.2E-03	4.6E-04	2.2E-03	4.4E-03	4.8E-03	1.3E-02	2.4E-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

注 1：此表给出了 PFD_G 的示例值，它是根据 B.3.1 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、逻辑或最终元件子系统分别对应一个表决组，则 PFH_G 分别等于 PFH_S、PFH_L 或 PFH_{FE}（见 B.3.2.1）。

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。

注 3：假设安全失效率等于危险失效率并且 $K=0.98$。

B.3.2.4 低要求运行模式示例

考虑一个安全功能要求为 SIL2 的系统。假设基于之前的经验，对系统架构的初始评估是用 1 组表决架构为 2oo3 的 3 个模拟压力传感器。逻辑子系统是配置为冗余 1oo2D 的 PE 系统，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.14 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一年。

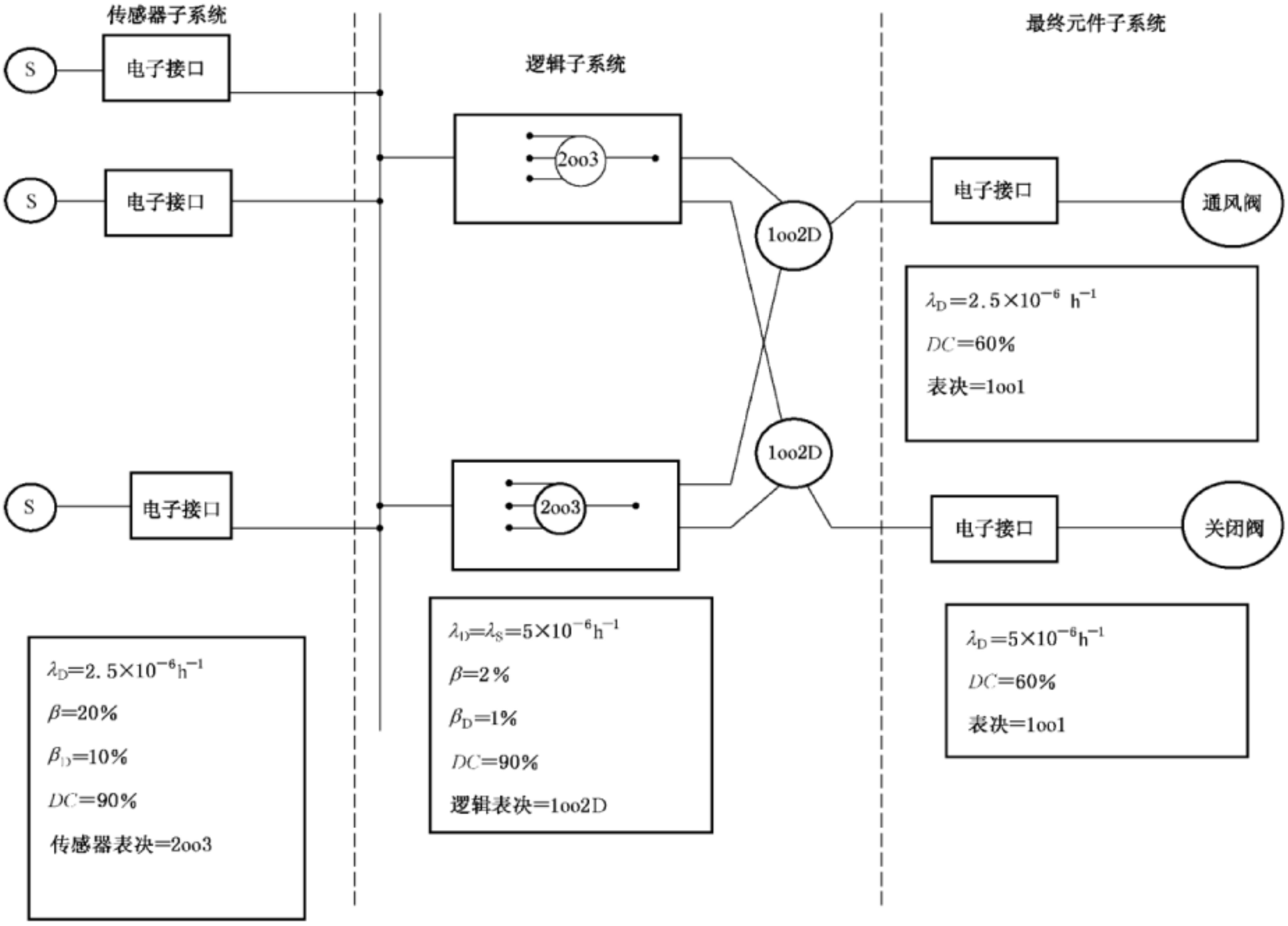


图 B.14 低要求运行模式架构示例

表 B.6 低要求运行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*	$\lambda_D=2.5E-06$		
		$\beta=2\%$ $\beta_D=1\%$	$\beta=10\%$ $\beta_D=5\%$	$\beta=20\%$ $\beta_D=10\%$
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　低要求运行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_D=0.5E-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　低要求运行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：

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

对于逻辑子系统：

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

对于最终元件子系统：

$$PFD_{FE} = 4.4\times10^{-3}+8.8\times10^{-3}$$
$$=1.3\times10^{-2}$$

因此,对于安全功能：

$$PFD_{SYS}=2.3\times10^{-4}+4.8\times10^{-6}+1.3\times10^{-2}$$
$$=1.3\times10^{-2}$$

属于安全完整性等级 1

为了改进系统使其满足安全完整性等级 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；

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

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

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

$PFD_{SYS}=6.7\times10^{-3}$

属于安全完整性等级 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%)

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

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

$PFD_{FE} = 4.4 \times 10^{-3} + 9.7 \times 10^{-4}$

$= 5.4 \times 10^{-3}$

$PFD_{SYS} = 5.6 \times 10^{-3}$

属于安全完整性等级 2

B.3.2.5 非完善检验测试的影响

在安全相关系统中的故障,既没有被诊断测试检测到又没有被检验测试检测到,而可能在要求安全功能动作的危险事件出现时或者设备检修时被发现。如在上述方法中,故障没有被发现,则应假设故障依然在设备的寿命中存在。假设正常的检验测试时间间隔周期为 T_1,其中,在检验测试中可以检出的故障百分比定义为 PTC(检验测试覆盖率),那么在检验测试中未被检出的故障百分比为$(1-PTC)$。对于在检验测试中未被检出的故障,他们仅能在要求之间的时间间隔 T_2 中要求安全相关系统动作时才可以被发现。因此,检验测试时间间隔周期(T_1)以及要求之间的时间间隔(T_2)决定了有效的不工作时间。

下面给出了 1oo2 架构的例子,T_2 为向系统提要求的间隔时间。

$$t_{CE} = \frac{\lambda_{DU}(PTC)}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DU}(1-PTC)}{\lambda_D}\left(\frac{T_2}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$t_{GE} = \frac{\lambda_{DU}(PTC)}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DU}(1-PTC)}{\lambda_D}\left(\frac{T_2}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$$

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

$$\beta\lambda_{DU}(1-PTC)\left(\frac{T_2}{2} + MRT\right)$$

表 B.9 给出了 1oo2 系统在检验测试时间间隔(T_1)为期一年的情况下 100%的检验测试与 90%的检验测试对比的数字结果,其中要求之间的时间间隔周期 T_2 假设为 10 年。此例在计算中还假设失效率为 0.5×10^{-5}/h,其中 β 为 10%,β_D 为 5%。

表 B.9 非完善检验测试的示例

架构	DC	$\lambda_D = 0.5$E-05	
		100%检验测试 $\beta = 10\%$ $\beta_D = 5\%$	90%检验测试 $\beta = 10\%$ $\beta_D = 5\%$
1oo2	0%	2.7E-03	6.0E-02
	60%	9.7E-04	2.0E-03
	90%	2.3E-04	4.4E-04
	99%	2.4E-05	4.4E-05

B.3.3 平均危险失效频率(对于高要求或连续运行模式)

B.3.3.1 计算的过程

高要求或连续运行模式下工作的 E/E/PE 安全相关系统安全功能的失效概率计算方法与低要求

运行模式的计算方法相同(见 B.2.1),只是用平均危险失效频率(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平均危险失效频率;

PFH_{S} ——传感器子系统平均危险失效频率;

PFH_{L} ——逻辑子系统平均危险失效频率;

PFH_{FE} ——最终元件子系统平均危险失效频率。

B.3.3.2 高要求或连续运行模式的架构

注 1:本条按顺序阅读,因为对几种架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 B.3.1 中的假设。

B.3.3.2.1 1oo1

图 B.4 与图 B.5 给出了相关的框图。

$$\lambda_{D}=\lambda_{DU}+\lambda_{DD}$$

$$t_{CE}=\frac{\lambda_{DU}}{\lambda_{D}}\left(\frac{T_{1}}{2}+MRT\right)+\frac{\lambda_{DD}}{\lambda_{D}}MTTR$$

$$\lambda_{DU}=\lambda_{D}(1-DC);\lambda_{DD}=\lambda_{D}DC$$

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

$$PFH_{G}=\lambda_{DU}$$

B.3.3.2.2 1oo2

图 B.6 与图 B.7 给出了相关的框图。t_{CE}为 B.3.3.2.1 中给出的值。如果假设在两个通道中只要有一个检测到失效时,安全系统将使 EUC 进入安全状态,并且采取保守方法,则可以得到如下公式:

$$PFH_{G}=2((1-\beta_{D})\lambda_{DD}+(1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU}t_{CE}+\beta\lambda_{DU}$$

B.3.3.2.3 2oo2

图 B.8 与图 B.9 给出了相关的框图。如果假设每个通道在检测到任何失效时,均使本通道进入安全状态,对于 2oo2 结构,则可以得到如下公式:

$$PFH_{G}=2\lambda_{DU}$$

B.3.3.2.4 1oo2D

图 B.10 与图 B.11 给出了相关的框图。

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

$$t_{CE}{}'=\frac{\lambda_{DU}\left(\frac{T_{1}}{2}+MRT\right)+(\lambda_{DD}+\lambda_{SD})MTTR}{\lambda_{DU}+\lambda_{DD}+\lambda_{SD}}$$

$$PFH_{G}=2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU}+(1-\beta_{D})\lambda_{DD}+\lambda_{SD})t_{CE}{}'+2(1-K)\lambda_{DD}+\beta\lambda_{DU}$$

B.3.3.2.5 2oo3

图 B.12 与图 B.13 给出了相关的框图。t_{CE}为 B.3.3.2.1 中的值。如果假设只有在任意两个通道同时检测到失效时安全系统将使 EUC 进入安全状态,并且采取保守方法,则可以得到如下公式:

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

B.3.3.2.6 1oo3

图 B.12 与图 B.13 给出了相关的框图。t_{CE}为 B.3.3.2.1 中的值,t_{GE}为 B.3.3.2.2 中的值。如果假设在三个通道中只要检测到一个失效,安全系统将使 EUC 进入安全状态,并且采取保守方法,则可以得到如下公式:

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

B.3.3.3 高要求或连续运行模式的详表

表 B.10 检验测试时间间隔为 1 个月、平均恢复时间为 8 h 的平均危险失效频率(高要求或连续运行模式下)

结构	DC	λ_D=0.5E-07			λ_D=2.5E-07			λ_D=0.5E-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%	4.0E-10	20E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
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 (见注 3)	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%	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90%	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99%	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-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%	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.1E-09	2.0E-08	4.0E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

表 B.10（续）

结构	DC	λ_D=0.5E-07			λ_D=2.5E-07			λ_D=0.5E-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%
1oo3	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%	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

结构	DC	λ_D=2.5E-06			λ_D=0.5E-05			λ_D=2.5E-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			> 1E-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%	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%	2.1E-08	1.0E-07	2.0E-07	4.3E-08	2.0E-07	4.0E-07	2.7E-07	1.1E-06	2.1E-06
	90%	5.1E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.5E-08	2.5E-07	5.0E-07
	99%	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08
2oo2 （见注 2）	0%	5.0E-06			1.0E-05			> 1E-05		
	60%	2.0E-06			4.0E-06			> 1E-05		
	90%	5.0E-07			1.0E-06			5.0E-06		
	99%	5.0E-08			1.0E-07			5.0E-07		
1oo2D （见注 3）	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%	8.1E-08	1.6E-07	2.6E-07	1.6E-07	3.2E-07	5.2E-07	8.7E-07	1.7E-06	2.7E-06
	90%	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.6E-07	1.2E-06	1.4E-06
	99%	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-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%	2.2E-08	1.0E-07	2.0E-07	4.9E-08	2.1E-07	4.1E-07	4.2E-07	1.2E-06	2.2E-06
	90%	5.2E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07	6.6E-08	2.6E-07	5.1E-07
	99%	5.2E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-07	5.4E-09	2.5E-08	5.0E-08
1oo3	0%	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	5.1E-07	2.5E-06	5.0E-06
	60%	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.0E-07	1.0E-06	2.0E-06
	90%	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99%	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

注 1：此表给出了 PFH_G 的示例值，它是根据 B.3.1 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、逻辑或最终元件子系统分别对应一个表决组，则 PFH_G 分别等于 PFH_S、PFH_L 或 PFH_{FE}（见 B.3.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均危险失效频率。

注 3：假设安全失效率等于危险失效率，$K=0.98$。

表 B.11　检验测试时间间隔为 3 个月，平均恢复时间为 8 h 的平均危险失效概率
（高要求或连续运行模式下）

结构	DC	λ_D=0.5E-07			λ_D=2.5E-07			λ_D=0.5E-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%	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.1E-09	2.0E-08	4.0E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
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 （见注 3）	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%	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90%	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99%	2.0E-09	2.0E-09	2.1E-09	1.0E-09	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-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%	4.0E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.3E-09	2.0E-08	4.0E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	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%	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

表 B.11（续）

结构	DC	λ_D=2.5E-06			λ_D=0.5E-05			λ_D=2.5E-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			> 1E-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%	2.2E-08	1.0E-07	2.0E-07	4.9E-08	2.1E-07	4.1E-07	4.2E-07	1.2E-06	2.2E-06
	90%	5.1E-09	2.5E-08	5.0E-07	1.1E-08	5.0E-08	1.0E-07	6.4E-08	2.6E-07	5.1E-07
	99%	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.2E-09	2.5E-08	5.0E-08
2oo2 （见注 2）	0%	5.0E-06			1.0E-05			> 1E-05		
	60%	2.0E-06			4.0E-06			> 1E-05		
	90%	5.0E-07			1.0E-06			5.0E-06		
	99%	5.0E-08			1.0E-07			5.0E-07		
1oo2D （见注 3）	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%	8.2E-08	1.6E-07	2.6E-07	1.7E-07	3.3E-07	5.3E-07	1.0E-06	1.8E-06	2.8E-06
	90%	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.6E-07	1.2E-06	1.4E-06
	99%	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	2.0E-06
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%	2.6E-08	1.1E-07	2.0E-07	6.6E-08	2.2E-07	4.2E-07	8.5E-07	1.6E-06	2.5E-06
	90%	6.4E-09	2.5E-08	5.0E-07	1.2E-08	5.1E-08	1.0E-07	9.3E-08	2.9E-07	5.3E-07
	99%	5.1E-10	2.5E-09	5.0E-07	1.0E-09	5.0E-09	1.0E-08	5.7E-09	2.6E-08	5.1E-08
1oo3	0%	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	5.5E-07	2.5E-06	5.0E-06
	60%	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.0E-07	1.0E-06	2.0E-06
	90%	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99%	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

注 1：此表给出了 PFH_G 的示例值，它是根据 B.3.1 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、逻辑或最终元件子系统分别对应一个表决组，则 PFH_G 分别等于 PFH_S、PFH_L 或 PFH_{FE}（见 B.3.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均危险失效频率。

注 3：假设安全失效率等于危险失效率，$K=0.98$。

表 B.12　检验测试时间间隔为 6 个月、平均恢复时间为 8 h 的平均危险失效概率
（高要求或连续运行模式下）

结构	DC	λ_D=0.5E-07			λ_D=2.5E-07			λ_D=0.5E-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%	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.2E-09	2.0E-08	4.0E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
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 （见注 3）	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%	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90%	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99%	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-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%	4.1E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.5E-09	2.0E-08	4.0E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	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%	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

表 B.12（续）

结构	DC	λ_D=2.5E-06			λ_D=0.5E-05			λ_D=2.5E-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			> 1E-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%	2.4E-08	1.0E-07	2.0E-07	5.7E-08	2.1E-07	4.1E-07	6.3E-07	1.4E-06	2.3E-06
	90%	5.3E-09	2.5E-08	5.0E-07	1.1E-08	5.1E-08	1.0E-07	7.8E-08	2.7E-07	5.2E-07
	99%	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08
2oo2 （见注 2）	0%	5.0E-06			1.0E-05			> 1E-05		
	60%	2.0E-06			4.0E-06			> 1E-05		
	90%	5.0E-07			1.0E-06			5.0E-06		
	99%	5.0E-08			1.0E-07			5.0E-07		
1oo2D （见注 3）	0%	7.6E-08	2.7E-07	5.2E-07	2.1E-07	5.9E-07	1.0E-06	3.1E-06	4.7E-06	6.8E-06
	60%	8.4E-08	1.6E-07	2.6E-07	1.8E-07	3.3E-07	5.3E-07	1.2E-06	2.0E-06	2.9E-06
	90%	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.8E-07	1.2E-06	1.4E-06
	99%	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-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%	3.3E-08	1.1E-07	2.1E-07	9.1E-08	2.4E-07	4.4E-07	1.5E-06	2.1E-06	2.9E-06
	90%	5.8E-09	2.6E-08	5.1E-08	1.3E-08	5.3E-08	1.0E-07	1.3E-07	3.2E-07	5.6E-07
	99%	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	6.1E-09	2.6E-08	5.1E-08
1oo3	0%	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	7.1E-07	2.7E-06	5.1E-06
	60%	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.1E-07	1.0E-06	2.0E-06
	90%	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99%	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

注 1：此表给出了 PFH_G 的示例值，它是根据 B.3.1 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、逻辑或最终元件子系统分别对应一个表决组，则 PFH_G 分别等于 PFH_S、PFH_L 或 PFH_{FE}（见 B.3.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均危险失效频率。

注 3：假设安全失效率等于危险失效率，$K=0.98$。

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 的平均危险失效概率
（高要求或连续运行模式下）

结构	DC	λ_D=0.5E-07			λ_D=2.5E-07			λ_D=0.5E-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		
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%	4.0E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.3E-09	2.0E-08	4.0E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
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 （见注 3）	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%	1.6E-09	3.2E-09	5.2E-09	8.1E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90%	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99%	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	0%	1.0E-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%	4.1E-10	2.0E-09	4.0E-09	2.3E-09	1.0E-08	2.0E-08	5.0E-09	2.1E-08	4.1E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.2E-10	2.5E-09	5.0E-09	1.1E-09	5.1E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	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%	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90%	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99%	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

表 B.13（续）

结构	DC	λ_D=2.5E-06			λ_D=0.5E-05			λ_D=2.5E-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			> 1E-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	5.2E-07	3.1E-07	6.8E-07	1.1E-06	5.8E-06	6.9E-06	8.5E-06
	60%	2.9E-08	1.1E-07	2.1E-07	7.4E-08	2.3E-07	4.2E-07	1.1E-07	1.7E-06	2.6E-06
	90%	5.5E-09	2.5E-08	5.0E-07	1.2E-08	5.2E-08	1.0E-07	1.0E-07	3.0E-07	5.4E-07
	99%	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.6E-09	2.6E-08	5.0E-08
2oo2 （见注 2）	0%	5.0E-06			1.0E-05			> 1E-05		
	60%	2.0E-06			4.0E-06			> 1E-05		
	90%	5.0E-07			1.0E-06			5.0E-06		
	99%	5.0E-08			1.0E-07			5.0E-07		
1oo2D （见注 3）	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%	8.9E-08	1.7E-07	2.7E-07	1.9E-07	3.5E-07	5.4E-07	1.7E-06	2.3E-06	3.2E-06
	90%	9.6E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	1.0E-07	1.2E-06	1.4E-06
	99%	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.6E-05	1.0E-06
2oo3	0%	2.1E-07	3.8E-07	6.1E-07	7.3E-07	1.0E-07	1.4E-06	1.6E-05	1.6E-05	1.6E-06
	60%	4.6E-08	1.2E-07	2.2E-07	1.4E-08	2.9E-07	4.7E-07	2.8E-06	3.2E-06	3.8E-06
	90%	6.6E-09	2.6E-08	5.1E-08	1.6E-08	5.6E-08	1.0E-07	2.1E-07	3.9E-07	6.2E-07
	99%	5.2E-10	2.5E-09	5.0E-09	1.1E-09	5.1E-09	1.0E-08	6.9E-09	2.7E-08	5.1E-08
1oo3	0%	5.1E-08	2.5E-07	5.0E-07	1.0E-07	5.1E-07	1.0E-06	1.4E-07	3.2E-06	5.5E-06
	60%	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.6E-07	1.0E-06	2.0E-06
	90%	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.1E-08	2.5E-07	5.0E-07
	99%	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

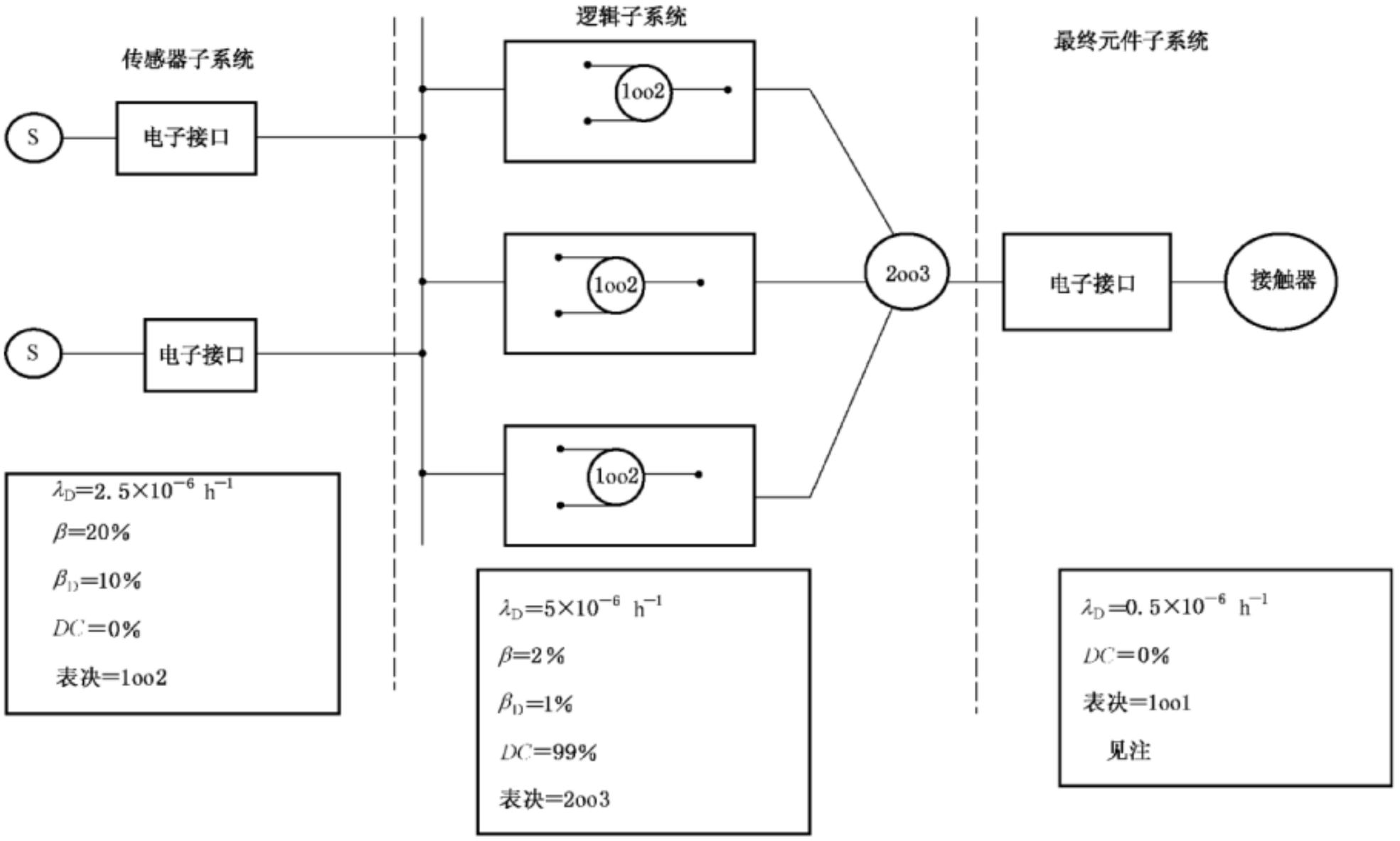
注 1：此表给出了 PFH_G 的示例值，它是根据 B.3.1 中所列出的假设，使用 B.3.2 中的公式计算出的，如果传感器、逻辑或最终元件子系统分别对应一个表决组，则 PFH_G 分别等于 PFH_S、PFH_L 或 PFH_{FE}（见 B.3.2.1）。

注 2：在此表中，假设 $\beta=2\times\beta_D$，对于 1oo1 和 2oo2 结构，β 和 β_D 的值不会影响平均危险失效频率。

注 3：假设安全失效率等于危险失效率，$K=0.98$。

B.3.3.4 高要求或连续运行模式的示例

考虑一个安全功能要求为 SIL2 的系统。假设基于之前的经验,对系统架构的初始评估是用 1 组表决架构为 1oo2 的 2 个传感器。逻辑子系统是配置为冗余 2oo3 的 PE 系统,用于驱动 1 个单独的停机接触器。如图 B.15 所示,初始评估时假设检验测试时间间隔为 6 个月。



注:最终元件子系统的总安全失效分数大于 60%。

图 B.15 高要求或连续运行模式的架构示例

表 B.14 高要求或连续运行模式架构示例中传感器子系统平均危险失效频率
(检验测试的时间间隔为 6 个月,*MTTR* 为 8 h)

结构	*DC*	λ_D=2.5E-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%	2.4E-08	1.0E-07	2.0E-07
	90%	5.3E-09	2.5E-08	5.0E-08
	99%	5.0E-10	2.5E-09	5.0E-09
注:此表摘自表 B.12。				

表 B.15　高要求或连续运行模式架构示例中逻辑子系统平均危险失效频率
（检验测试的时间间隔为 6 个月，*MTTR* 为 8 h）

结构	*DC*	λ_D=0.5E-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%	9.1E-08	2.4E-07	4.4E-07
	90%	1.3E-08	5.3E-08	1.0E-07
	99%	1.0E-09	5.3E-09	1.0E-08
注：此表摘自表 B.12。				

表 B.16　高要求或连续运行模式架构示例中最终元件子系统平均危险失效频率
（检验测试的时间间隔为 6 个月，*MTTR* 8 h）

结构	*DC*	λ_D=0.5E-06
1oo1	0%	5.0E-07
	60%	2.0E-07
	90%	5.0E-08
	99%	5.0E-09
注：此表摘自表 B.12。		

从表 B.14～表 B.16 中可获得出下列数值。

对于传感器子系统

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

对于逻辑子系统

$PFH_L = 1.0\times10^{-9}/h$

对于最终元件子系统

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

因此，对于安全功能

$PFH_{SYS} = 5.2\times10^{-7} + 1.0\times10^{-9} + 5.0\times10^{-7}$

$= 1.02\times10^{-6}/h$

属于安全完整性等级 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%。

$PFH_S = 2.7\times10^{-7}/h$

$PFH_L = 1.0\times10^{-9}/h$

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

$PFH_{SYS} = 7.7\times10^{-7}/h$

属于安全完整性等级 2

b）　在 1oo2 中将单一输出设备改变为两个设备（β=10%、β_D=5%）

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

$PFH_L = 1.0 \times 10^{-9}/\text{h}$

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

$PFH_{SYS} = 5.7 \times 10^{-7}/\text{h}$

属于安全完整性等级 2

B.4 布尔方法

B.4.1 概述

布尔方法包含的技术描述了单个部件失效与整体系统失效相联系的逻辑关系。在可靠性领域使用的主要布尔模型是:可靠性框图(RBD)、故障树(FT)、事件树和因果关系图,这里我们仅考虑前两种模型。所有模型的目的都是为了描述系统的逻辑结构。但是这些模型技术不描述系统随时间的运行行为。因此,当需要考虑计算系统运行指标时(例如与时间相关的周期性检验测试间隔),就要小心。使用布尔模型的第一步是将图形描述与计算分离开。这在前面章节做出了说明,其中 RBD 是用来对结构建模,马尔可夫计算则是用来评估 PFD 或者 PFH。下面讨论在 RBD 和 FT 基础上做概率计算。

这个方法限定部件之间的运行需保持相互合理的独立性。

B.4.2 可靠性框图模型

前面给出了很多 RBD 的例子,图 B.1 描述了一个完整的安全回路,其中回路由 1oo3 结构的三个传感器(A、B、C)、一个逻辑运算器(D)和 1oo2 结构的两个最终元件(E、F)组成。

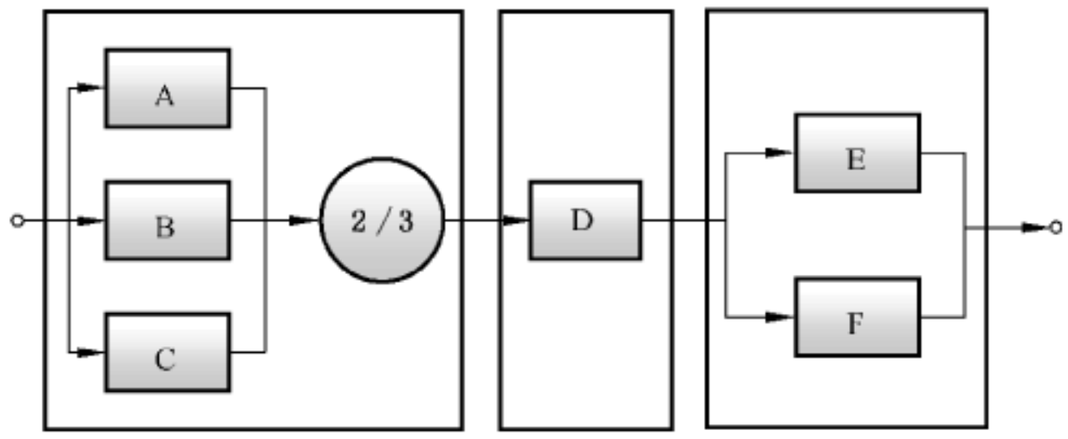


图 B.16 带有 2oo3 结构传感器的简单完整的回路的可靠性框图

图 B.16 是一个类似回路,其中传感器为 2oo3 结构。这种框图的描述方法主要关注三个方面:它非常接近系统的真实物理结构;它被工程师广泛使用;它给讨论提供了很好的支持。

RBD 的主要缺点是,与其说它是一种分析方法不如说是一种描述方法。

RBD 的更多细节见 GB/T 20438.7—2017 中 C.6.4 和 IEC 61078。

B.4.3 故障树模型

故障树模型与 RBD 有着几乎完全一样的特点,只是它增加了一个有效的演绎(自顶向下)分析方法,这个方法可以帮助可靠性工程师从顶部事件(非必要或者非预期事件)到单个部件失效,逐步的开发建立模型。

图 B.17 描述的故障树完全等效于图 B.1 中的 RBD 模型,除了要确定出自顶向下的分析步骤。(例如:E/E/PE 安全相关系统失效≥传感器失效≥传感器 A 失效)。在故障树中,串联元件用“或门”连接,并联元件(即冗余)用“与门”连接。

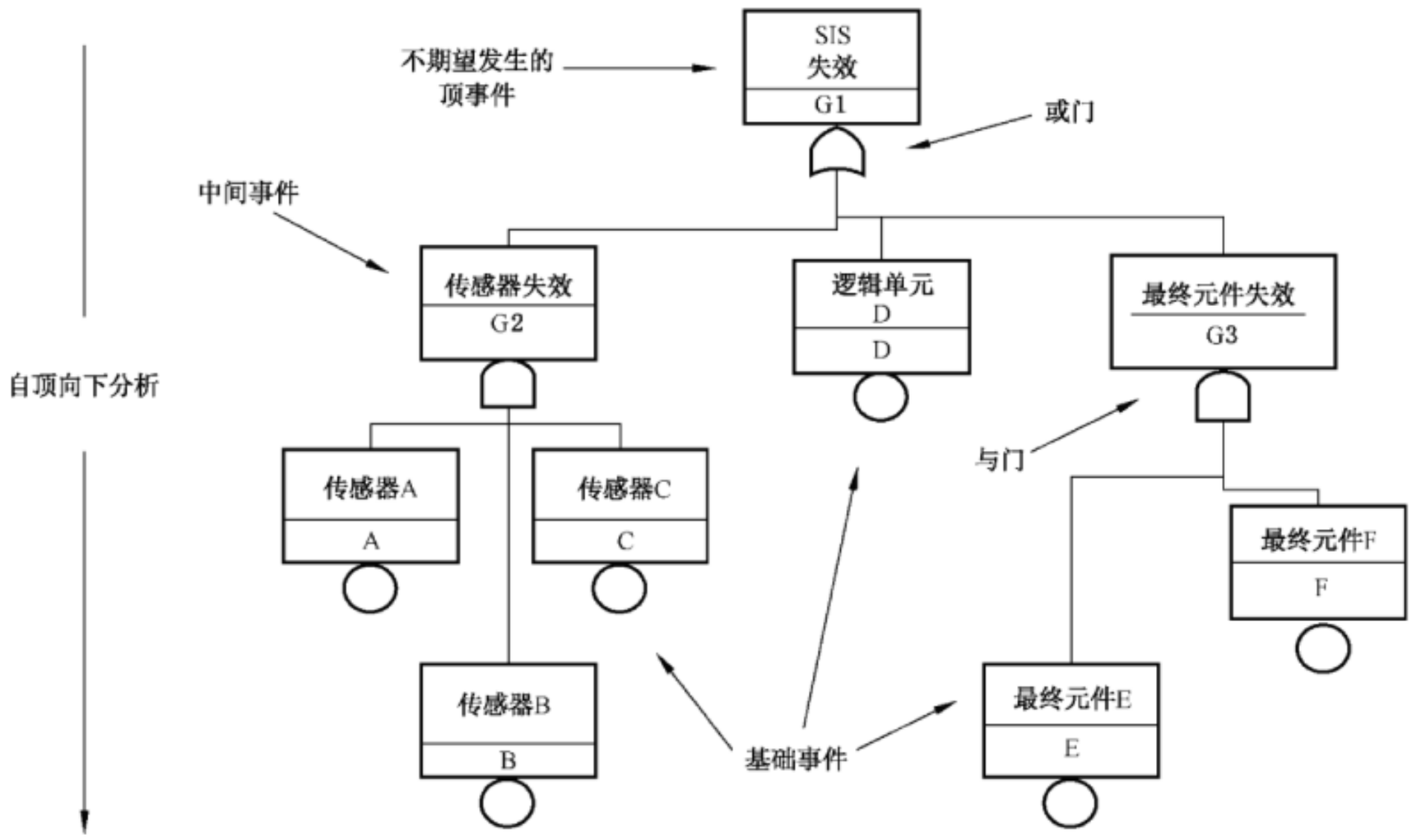


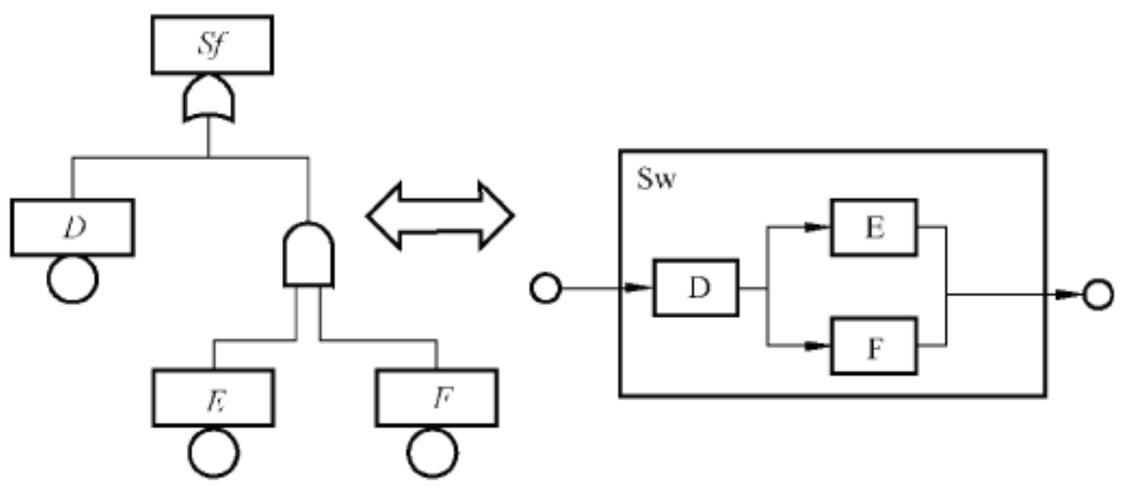
图 B.17　与可靠性框图 B.1 等效的简单故障树模型

FT 的更多细节见 GB/T 20438.7—2017 的 B.6.6.5 及 B.6.6.9 和 IEC 61025。

B.4.4　PFD 计算

B.4.4.1　概述

RBD 和 FT 可以确切描述同一事件，也可以采取同一方式进行计算。图 B.18 用较小规模的 FT 和 RBD 说明了计算的一些主要原理。



注：在本图中，斜体字表示失效项，非斜体字表示工作项。

图 B.18　等效故障树/可靠性框图

FT 描述的逻辑功能为 $Sf = D \cap (E \cup F)$，其中 Sf 代表系统失效，D、E、F 代表单个部件失效。RBD 描述的逻辑功能为 Sw＝D∪(E∩F)，其中 Sw 代表系统功能正常，D、E、F 代表单个部件功能正常。那么 Sf ＝NOT Sw，并且 Sf 和 Sw 描述了同样信息(即逻辑功能和它的两种表达方式)。

FT 和 RBD 的基本用法是来确定导致整体系统失效的不用部件的失效组合。这些失效组合之所以被称为最小割集是因为当他们在这个位置割断 RBD 时，输入信号将不能到达输出。在本例中，有两个最小割集：单个失效(D)和二重失效(E，F)。

对逻辑功能使用基本的概率算法可以直接得到系统失效概率 P_{Sf}，公式如下：

$$P_{Sf} = P(D) + P(E \cap F) - P(D \cap E \cap F)$$

如果部件是独立的，公式可化为：

$$P_{Sf} = P_D + P_E P_F - P_D P_E P_F$$

式中：

P_i——部件 i 的失效概率。

这个公式是与时间无关的而且仅反应了系统逻辑结构。

因此 RBD 和 FT 本质上都是静态的，即是与时间无关的模型。

另外，如果无论其他部件在$[0,t]$上处于何种状态，每个各单独部件在时刻 t 的失效概率都是与之相互独立的，那么上面公式在任意时刻都保持有效，可以写为：

$$P_{Sf}(t) = P_D(t) + P_E(t)P_F(t) - P_D(t)P_E(t)P_F(t)$$

分析人员需要验证所需的近似条件是否可以接受，最后得出，系统的瞬时不可用率 $U_{Sf}(t)$ 为：

$$U_{Sf}(t) = U_D(t) + U_E(t)U_F(t) - U_D(t)U_E(t)U_F(t)$$

结论是故障树或可靠性框图可以直接计算出 E/E/PE 安全相关系统的瞬时不可用率 $U_{Sf}(t)$，需要进行的附加计算依据 B.2.2：

$$PFD_{avg}(T) = \frac{1}{T}MDT(T) = \frac{1}{T}\int_0^T U_{Sf}(t)\,dt$$

最小割集可以计算如下：

——单个失效(D)：
$$PFD^D(\tau) = \frac{1}{\tau}\int_0^T \lambda_D t\,dt = \lambda_D \tau/2$$

——二重失效(E,F)：
$$PFD^{EF}(\tau) = \frac{1}{\tau}\int_0^T \lambda_E \lambda_F t^2\,dt = \lambda_E \lambda_F \tau^2/3$$

B.4.4.2 基于故障树或者可靠性框图工具的计算

上面公式 $U_{Sf}(t)=U_D(t)+U_E(t)U_F(t)-U_D(t)U_E(t)U_F(t)$ 仅仅是庞加莱(Poincare)公式的一个特殊情况，通常情况下，如果 $Sf=\bigcup_i C_i$，其中(C_i)代表系统的最小隔集，则有：

$$P\left(\bigcup_{i-1}^{n} C_i\right) = \sum_{j=1}^{n} P(C_j) - \sum_{j=1}^{n}\sum_{i=1}^{j-1} P(C_j \cap C_i) + \sum_{j=3}^{n}\sum_{i=2}^{j-1}\sum_{k=1}^{j-1} P(C_j \cap C_i \cap C_k) - \cdots$$

当单个部件数量增加时，最小隔集数量会以指数数量级别增加。这样庞加莱(Poincare)公式就会导致项目的组合计算高度复杂，用手算难以处理。幸运的是，过去四十年一直在分析这个问题，为处理这样的计算已经设计了很多算法。目前，最新开发的有力工具是基于二元判定框图(BDD)，其中 BDD 是由对逻辑关系的香农(Shannon)分解演进而来的。

主要基于故障树模型的大量商业软件，已被可靠性工程师广泛使用在各种不同的工业领域(核电、石油、航空、汽车等等)。商业软件可以用来计算 PFD_{avg}，但是分析人员必须要小心，因为其中一些商用软件执行了错误的 PFD_{avg} 计算。遇到的主要错误是，将单个部件的 PFD_{avg}，i(通常由 $\lambda_i\tau/2$ 得到)组合生成的结果做为整个系统的 PFD_{avg}，这种做法是错误而且是非保守的。

不管怎样，故障树软件可以用系统部件的瞬时不可用率 $U_i(t)$ 来计算系统的瞬时不可用率 $U_{sf}(t)$，可以用 $U_{sf}(t)$ 在关注时间段上的平均值来评估 PFD_{avg} 值，计算可由在使用中的软件或者其他方法来完成。

理想情况如图 B.19 中左图所示：

$$U_i(t) = \lambda\zeta,\ \zeta \text{ 为 } t \text{ 除以 } \tau \text{ 的余数}$$

图中锯齿形曲线以线性方式从 0 上升到 $\lambda\tau$，然后在一次测试或者修复(由于考虑 EUC 在此期间的停机是短暂的)之后又从 0 重新开始。

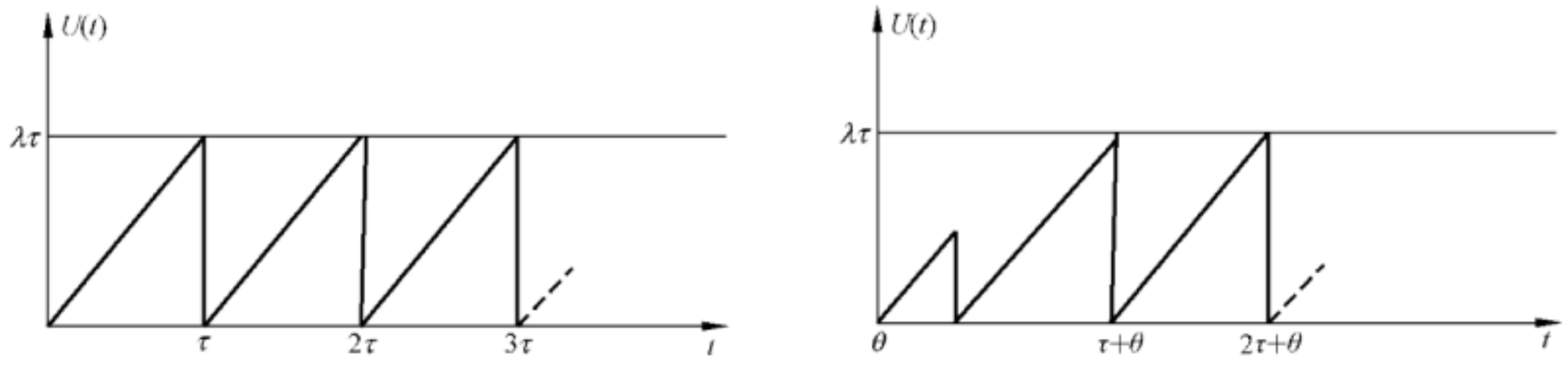


图 B.19　单一周期测试部件瞬时不可用率 $U(t)$

如有多个部件用在冗余结构中，当首次测试时间间隔与其他不同，如图 B.19 中右图所示，则测试会发生交错。这不会对 PFD_{avg} 值有影响，对两种情况下的最大值 $\lambda\tau/2$ 和 $\lambda\tau$ 也不会有影响。

当然在一些不理想的情况下，锯齿形曲线可能比理想情况要复杂很多。在 B.5.2 中给出了设计较精确锯齿波曲线的指导方法，但是对于本节来说，图 B.19 中的波形已经足够充分了。

这种方法可以应用到图 B.18 所示小型故障树模型中，具体描述见图 B.20（其中 DU 代表未检测出的危险，CCF 代表共因失效）。我们考虑由两个冗余部件（E，F）组成的系统，（D）是这些部件的共因失效。计算数据要求如下：

$$\lambda_{DU}=3.5\times10^{-6}/\mathrm{h},\tau=4380\mathrm{h},\beta=1\%$$

选取较小的 β 因子可以保证 CCF 不会主导顶事件的结果，并且方便更好理解其工作原理。

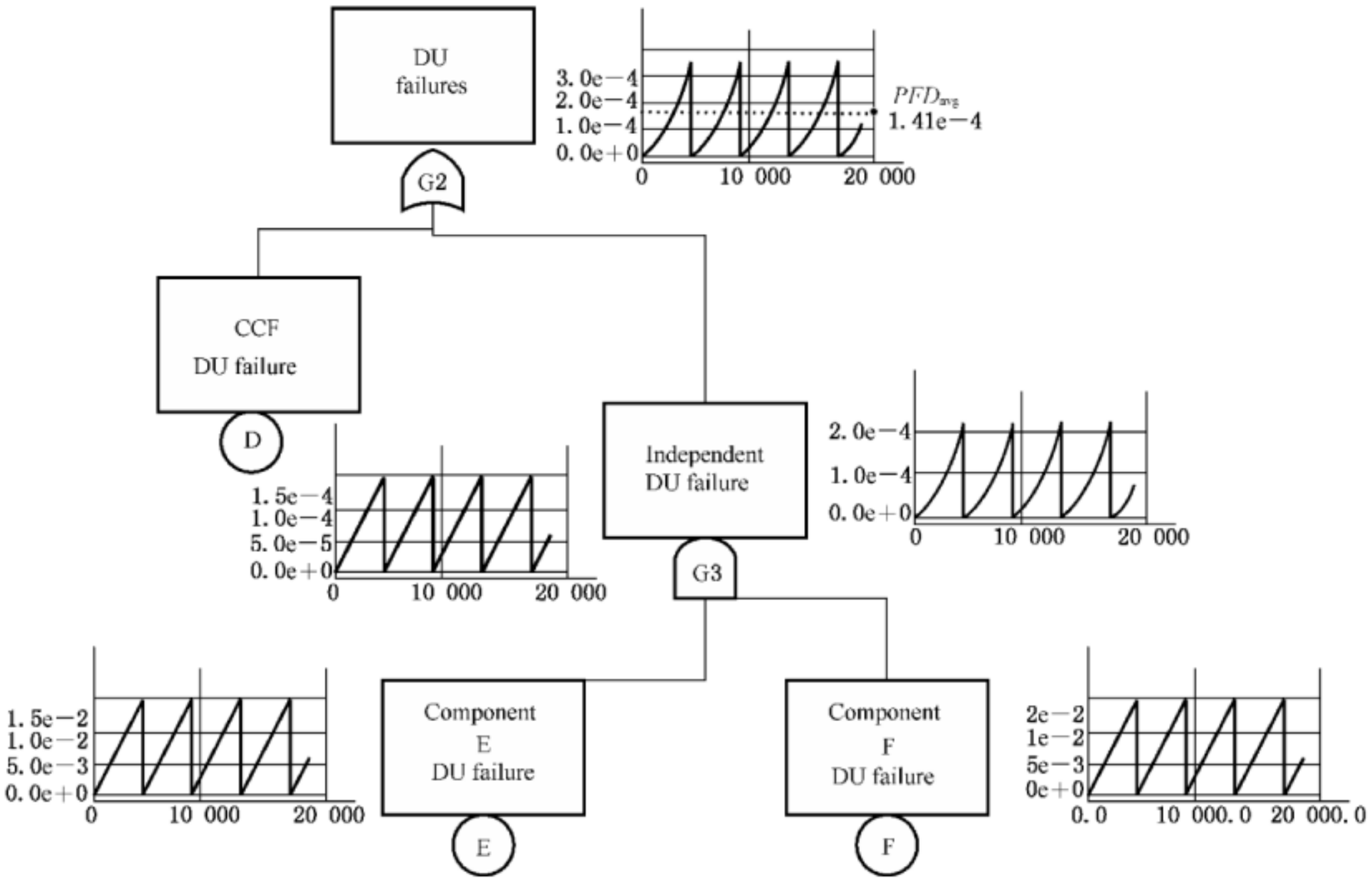


图 B.20　使用故障树时的 PFD_{avg} 计算原理

图 B.20 中左边的锯齿形曲线是容易识别的，其输入为 D、E、F。当对 E 或 F 的测试时，对 CCF（D）也测试一次。因此，如果 E 和 F 的测试时间间隔都是六个月，那么 CCF（D）的测试时间间隔同样也是六个月。

使用故障树计算的算法，很容易绘制出所有逻辑门输出的锯齿形曲线。PFD_{avg}是顶层事件结果的平均值，它可以通过故障树软件本身或者手工计算得出。计算得到 $PFD_{avg}=1.4\times10^{-4}$，依据GB/T 20438，满足了低要求操作模式SIL 3的目标失效要求。

如图B.20所示，测试曲线表现平稳，那么对于评估平均值没有困难，此处假设试验状态是确定的并且试验在预期中进行。

有一个有趣的现象，一旦执行冗余，测试中的顶部事件锯齿形曲线就不再是线性（即总的系统失效率不再是常数）。

当使用冗余部件交错测试代替同时测试来衡量对 PFD_{avg} 的影响时，也同样有趣。具体说明见图B.21，其中对部件F的测试与对部件E的测试交错时间为3个月。

这会产生如下重要影响：

——CCF现在是每隔3个月测试（即E每次测试时间和F每次测试时间）。这个检验测试频率是之前的两倍。

——顶层事件锯齿形曲线的检验测试频率也同样是之前的两倍。

——锯齿形曲线比之前围绕平均值的振幅减小。

——PFD_{avg}值降至 3.5×10^{-6}，依据新的测试方法，系统达到SIL 4。

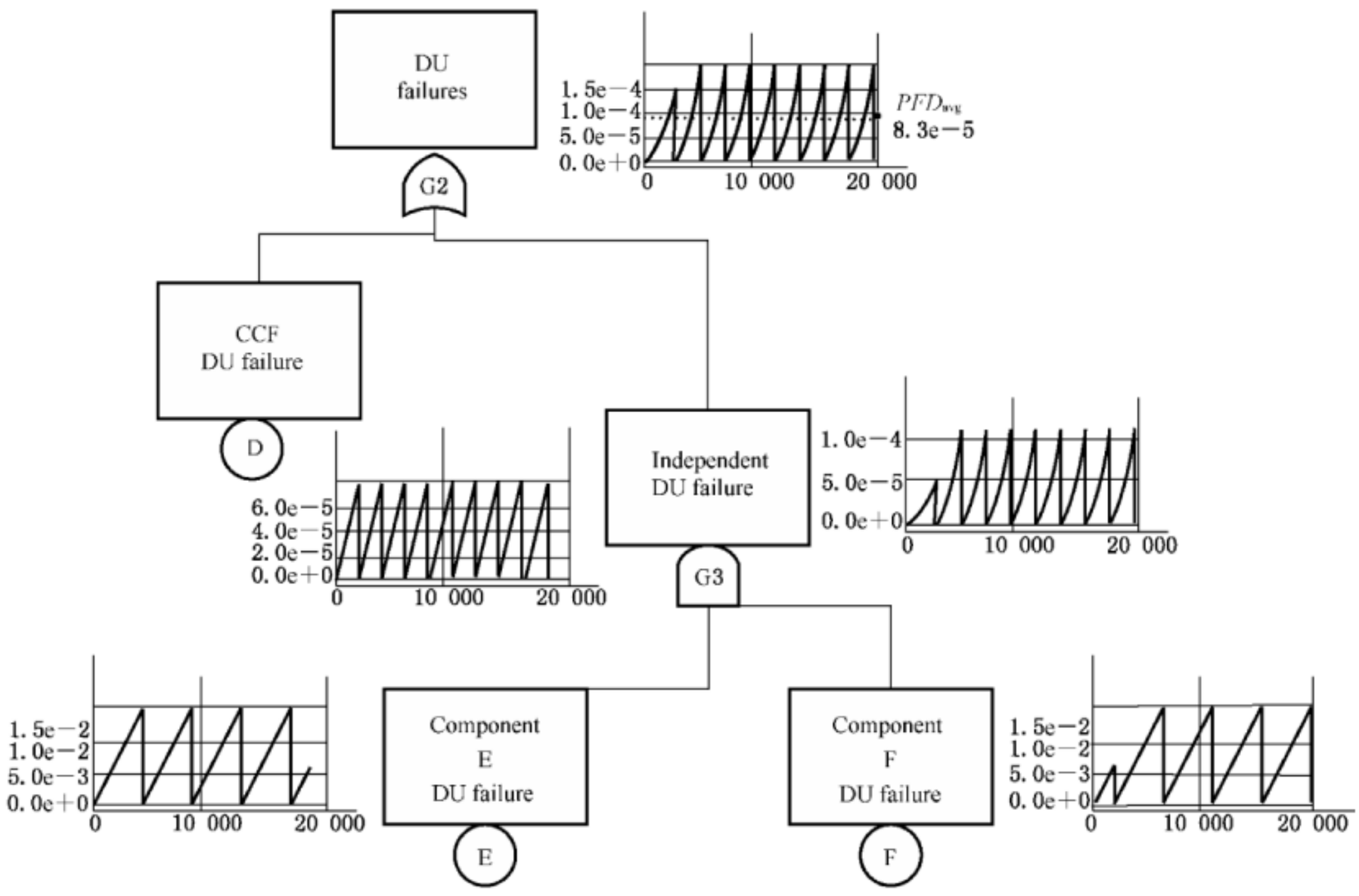


图 B.21　交错测试的影响

如果测试是交错的并按正确的步骤执行，将提高检测到CCFs的可能性，并且这是一个减少系统工作于低要求操作模式下CCF的有效方法。这样系统就从SIL 3提升到了SIL 4（针对硬件失效，并且满足了GB/T 20438的其他要求）。

图B.22描述了在图B.20系统建模中增加串联方式连接的组件G（$\lambda_{DU}=7\times10^{-9}$/h，不检测）和H（$\lambda_{DU}=4\times10^{-8}$/h，每两年检测一次）后得到的锯齿形曲线。

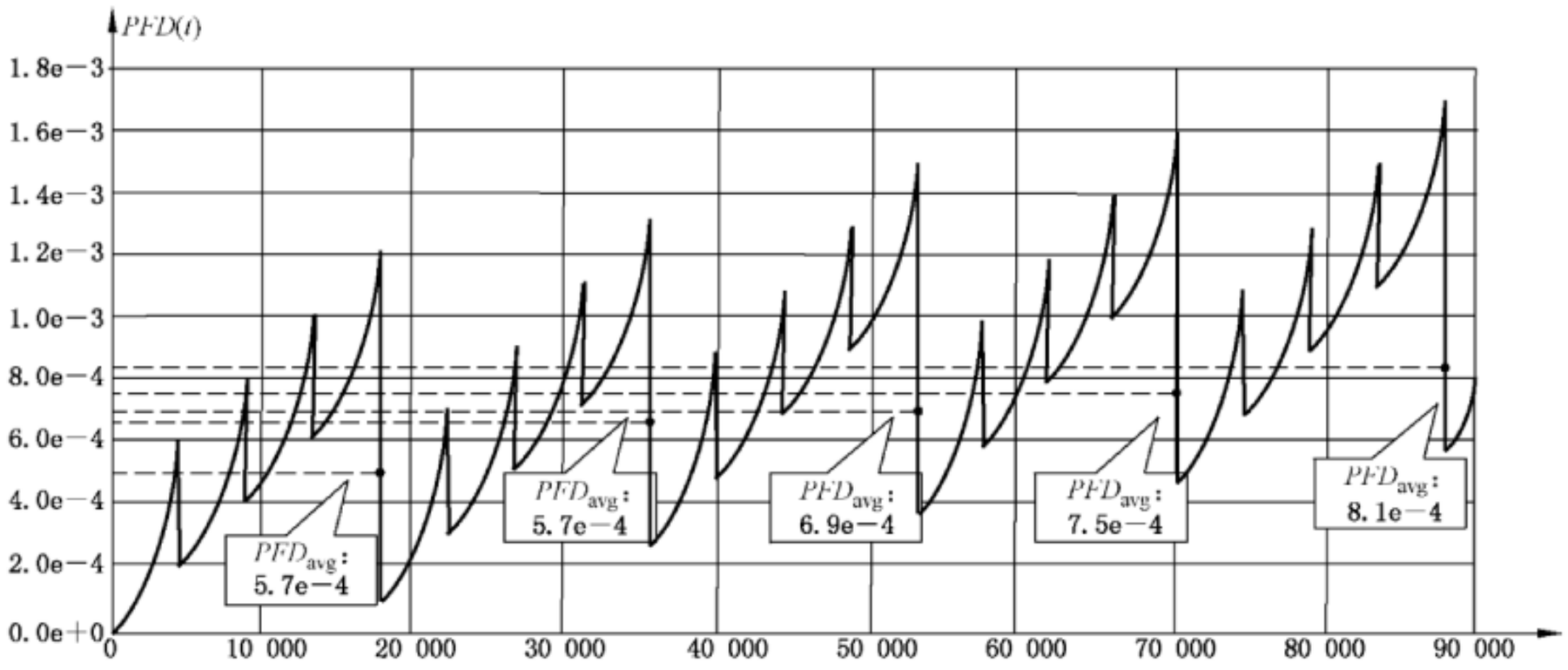


图 B.22　复杂测试模式实例

对组件 G 从不进行检测，会产生两方面的影响：$PFD(t)$每两年检测后都不归零并且 PFD_{avg} 持续增加(黑色圆圈代表的是虚线所覆盖时间内所对应的 PFD_{avg} 值)。

即使基本的锯齿形曲线(类似图 B.19)非常简单，顶层事件的结果也可能相当复杂，但是这不会增加特别的难度。

B.4 仅是为了阐明布尔模型的计算原理。B.5.2 与马尔可夫方法有关，将给出针对基本组件设计更先进输入锯齿形曲线的指导。

归纳如下：当单个部件独立时，使用通常的布尔技术来计算 E/E/PE 安全相关系统的 PFD_{avg} 值是没有问题的。从理论的角度来看这不简单，做这项研究的分析师需要具备大量的概率计算知识来识别和排除时常遇到的错误 PFD_{avg} 结果。假设采取了这些预防措施，任何故障树软件包都可以用于上述计算。

布尔技术也可以用于计算 PFH，但是其理论发展不列为本非规范性附录讨论范围。

B.5　状态/转移方法

B.5.1　总述

布尔模型本质上与时间无关，只有在特定情况下才能够引入时间的因素。这具有一定的人为因素，并且需要较好掌握概率方面知识以避免错误。因而，也可以采用其他本质上具有动态属性的概率模型。从可靠性方面讲，这些模型基本上是基于以下方法，其分为两个步骤：

——识别所研究的系统的全部状态；

——根据系统在生命周期内出现的事件，分析系统状态的跳变(或转移)

这就是为什么这些模型属于状态/转移模型的原因。

实际上，一般方法是：当出现失效、维修、测试等事件时，建立一种与所研究系统一样的自动化行为的描述。根据 GB/T 20438，E/E/PE 安全相关系统只存在不连续的状态，这相当于建立一种所谓的有限状态自动机。这些模型从本质上说是动态的，并可以通过很多种方法来实现：图示法、特定的形式化语言或通用编程语言。本附录介绍了两种方法，这两种方法有很大差异，但又互为补充。

——在 20 世纪初提出的马尔可夫模型。这种方法广为人们所熟悉，其采用分析式处理方法。

——20 世纪 60 年代提出的佩特里(Petri)网模型。熟悉这种模型的人不多(但是由于使用比较灵活，使用这种模型的人也越来越多)，其运用蒙特卡罗(Monte Carlo)模拟法进行建模。

这两种方法都是基于图形的方法，对用户很有帮助。在本章节结束部分还将简要分析其他基于形

式化语言模型的方法。

B.5.2 马尔可夫方法

B.5.2.1 建模原理

在可靠性领域,马尔可夫方法可以说是所有动态方法中最早的一种方法。马尔可夫过程可以分为两种,第一种是"无记忆的"(齐次马尔可夫过程,其中所有转移率均为常数),第二种是其他类别(半马尔可夫过程)。由于齐次马尔可夫过程的将来不依赖于它的过去,其解析计算相对简单。但对于半马尔可夫过程来说,计算就比较困难,这可用蒙特卡罗模拟法进行计算。在 GB/T 20438 的本部分中,只考虑齐次马尔可夫过程,而本文简称为"马尔可夫过程"(详见 GB/T 20438.7—2017 的 C.6.4 和 IEC 61165)。

马尔可夫过程的基本公式如下:

$$P_i(t+\mathrm{d}t)=\sum_{k\neq i}P_k(t)\lambda_{ki}\,\mathrm{d}t+P_i(t)\left(1-\sum_{k\neq i}\lambda_{ik}\,\mathrm{d}t\right)$$

其中,λ_{ki} 表示从状态 i 到状态 k 的转移率(如失效率或修复率)。显然:在 $t+\mathrm{d}t$ 之间处于状态 i 的概率即为向 i 跳变的概率(当处于另外一个状态 k 时)或在 t 和 $t+\mathrm{d}t$ 之间仍保持在状态 i 的概率(如果已处在状态 i 中)。

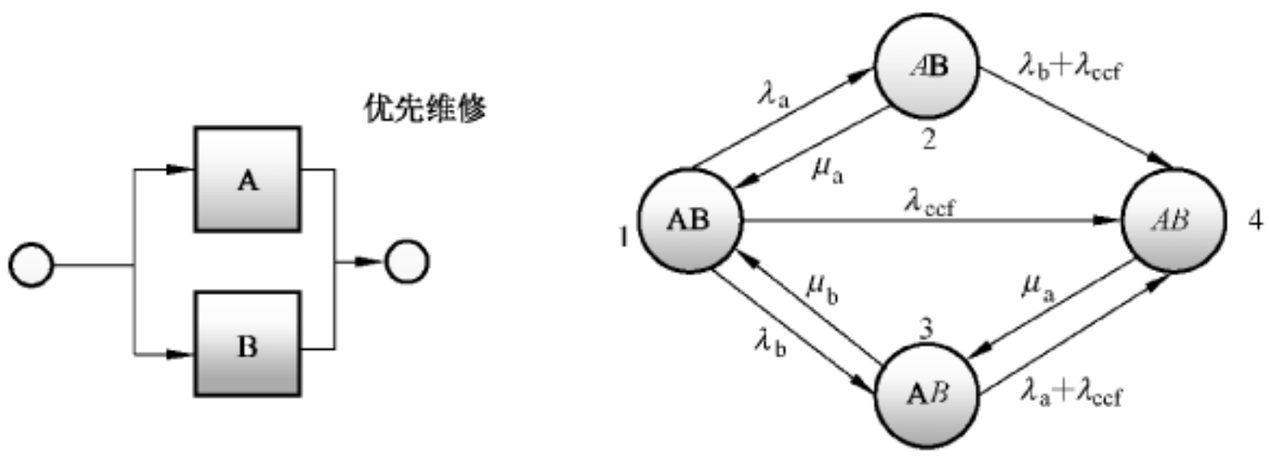


图 B.23 对一个双部件系统的马尔可夫图形建模

可以将上面的公式与图形化表示建立起一种直接的联系,如图 B.23 所示,其对一个双部件系统进行建模,该系统共用一个维修小组(部件 A 有优先维修权)并具有共因失效。在上图中,**A** 表示正常工作,*A* 表示已出现故障。由于必须考虑检测的时间,图中所示 μ_a 和 μ_b 都表示部件的修复率(如 $\mu_a=1/MTTR_a$ 和 $\mu_b=1/MTTR_b$)。

例如状态 4 的概率计算公式如下:

$$P_4(t+\mathrm{d}t)=[P_1(t)\lambda_{ccf}+P_2(t)(\lambda_b+\lambda_{ccf})+P_3(t)(\lambda_a+\lambda_{ccf})]\mathrm{d}t+P_4(t)(1-\mu_a\,\mathrm{d}t)$$

从而可以导出一个向量微分方程:

$\mathrm{d}\vec{P}(t)/\mathrm{d}t=[M]\vec{P}(t)$,其通常情况下的解如下:

$$\vec{P}(t)=\mathrm{e}^{t[M]}\vec{P}(0)$$

其中

$[M]$为包含转移率的马尔科夫矩阵,$\vec{P}(0)$为初始条件向量(通常为一个列向量,完好状态为 1,其他状态为 0)。

尽管矩阵指数的属性与普通指数不完全相同,也可以得出如下结论:

$$\vec{P}(t)=\mathrm{e}^{(t-t_1)[M]}\mathrm{e}^{t_1[M]}\vec{P}(0)=\mathrm{e}^{(t-t_1)[M]}\vec{P}(t_1)$$

这描述了马尔可夫过程的基本属性:给定 t_1 时刻的状态概率概括了所有过去演变的相关信息,并足以用来计算从 t_1 时刻起系统的未来是如何演变的。这个属性对于计算 *PFD* 非常有用。

很久以前人们就开发了高效的算法软件包,来求解上述方程。这样,在应用该方法时,分析人员可

以只关注于模型的构建，而不是基础的数学运算。不过，他至少应该理解本附录所介绍的方法原理。

图 B.24 显示了 *PFD* 计算原理：

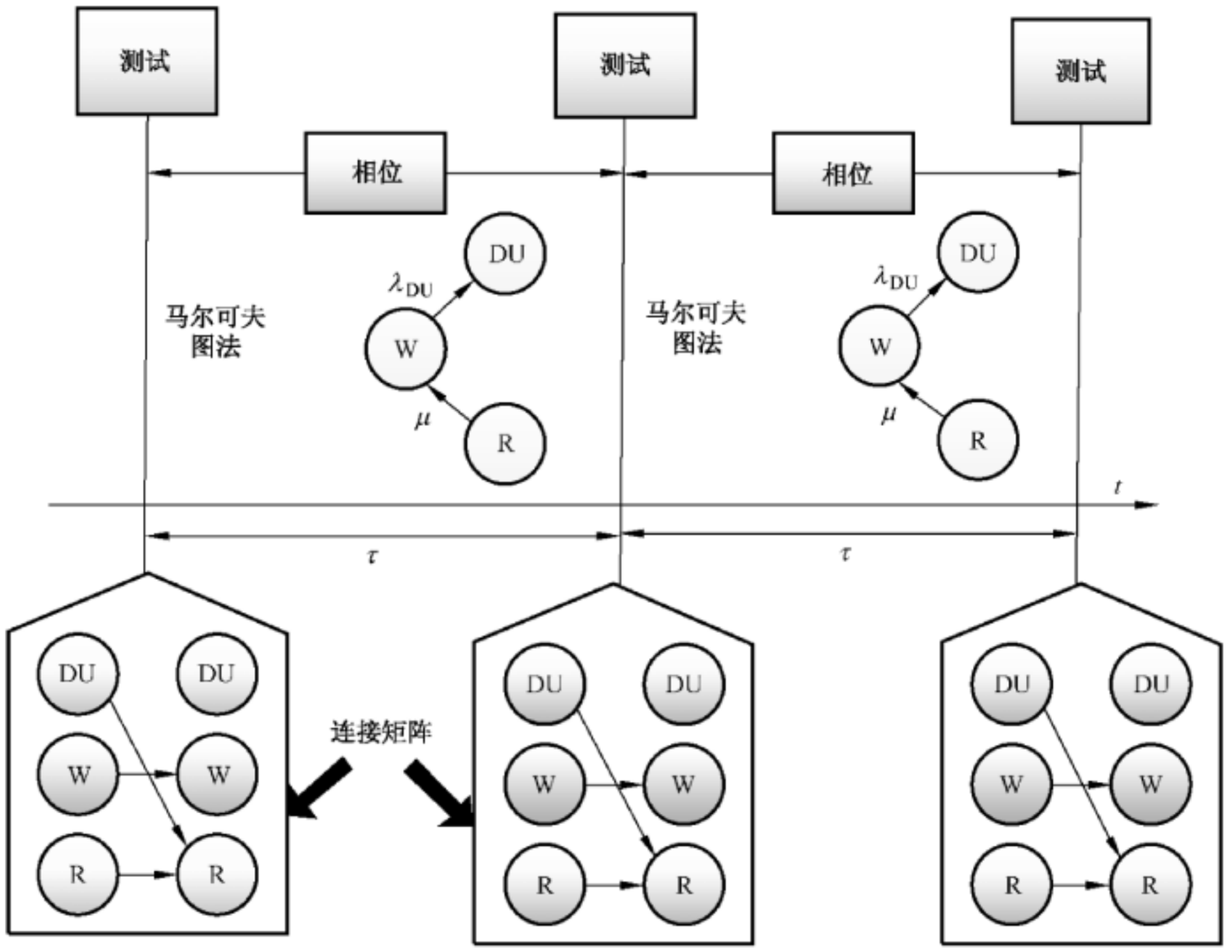


图 B.24　多相马尔可夫建模原理

PFD 计算与低要求运行模式中运行的、需要定期（检验）测试的 E/E/PE 安全相关系统有关。对于此类系统，只能在进行测试时才可以进行维修。这些测试是沿着时间的奇异点，但这不会成为一个问题，因为可以通过多相马尔可夫方法解决。

例如，一个由单个定期测试部件构成的简单系统拥有三种状态，如图 B.24 所示：正在运行（W），未能检测的危险失效（DU）和在维修中（R）。

在这些测试过程之间，系统行为可以通过马尔可夫过程进行建模，见图 B.24 上半部分：系统可能失效（W→DU）或在修理中（R→W）。由于在测试间隔内不会进行维修动作，DU 不会转移至 R。由于进入状态 R 之前已经进行失效诊断，图 B.24 中的 μ 表示部件的修复率（例如：$\mu=1/MRT$）。

当进行测试时（见图 B.14 的连接矩阵），如果出现失效（DU→R），就会开始维修而如果系统处于良好的功能状态（W→W），则部件保持运行状态。在一个非常极端的假设情形下，即在之前的测试尚未完成时就开始维修，则部件继续保持在维修状态（R→R）。通过连接矩阵[L]可以用测试 i 结束时的状态概率来计算状态 $i+1$ 开始阶段的初始条件。从而得出下列方程：

$$\begin{pmatrix} P_{DU}(0) \\ P_{W}(0) \\ P_{R}(0) \end{pmatrix}_{i+1} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{pmatrix} P_{DU}(\tau) \\ P_{W}(\tau) \\ P_{R}(\tau) \end{pmatrix}_{i} = \overrightarrow{P_{i+1}}(0) = [L]\,\overrightarrow{P_{i}}(\tau)$$

用$\overrightarrow{P_i}(\tau)$的值带入上式，可以得出一个递推方程，其可用于计算各个测试间隔开始阶段的初始条件：

$$\vec{P}_{i+1}(0) = [L]e^{t[M]}\,\vec{P}_{i}(0)$$

由此可以计算任何时间 $t=i\tau+\xi$ 的概率。例如在测试间隔 i 内，可得：

$$\vec{P}(t) = \vec{P}_{i}(\zeta) = e^{\zeta[M]}\,\vec{P}_{i}(0), (i-1)\tau \leqslant t < i\tau, \zeta = t \bmod \tau$$

通过对系统处于不可用状态概率的求和，可以直接得出瞬时不可用率。其可用线性矢量(q_k)表达为：

$$U(t)=\sum_{k=1}^{n}q_kP_k(t)$$

其中，如果系统在状态 k 时为不可用，则 $q_k=1$，在其他情况下 $q_k=0$。

对于一个简单模型，可得 $PFD(t)=U(t)=P_{DU}(t)+P_R(t)$，图 B.25 显示出该模型的锯齿形曲线走势。

通过前面所述的方法可利用 MDT 计算 PFD_{avg}，反过来也可以通过状态平均累积时间(MCT)进行计算：

$$\overrightarrow{MCT}(T)=\int_0^T\vec{P}(t)\,\mathrm{d}t$$

对于 $\vec{P}(t)$，使用已有的成熟算法进行$[0,T]$间的积分运算，最后可得：

$$PFD_{avg}(T)=\frac{1}{T}\sum_{k=1}^{n}q_kMCT_k(T)$$

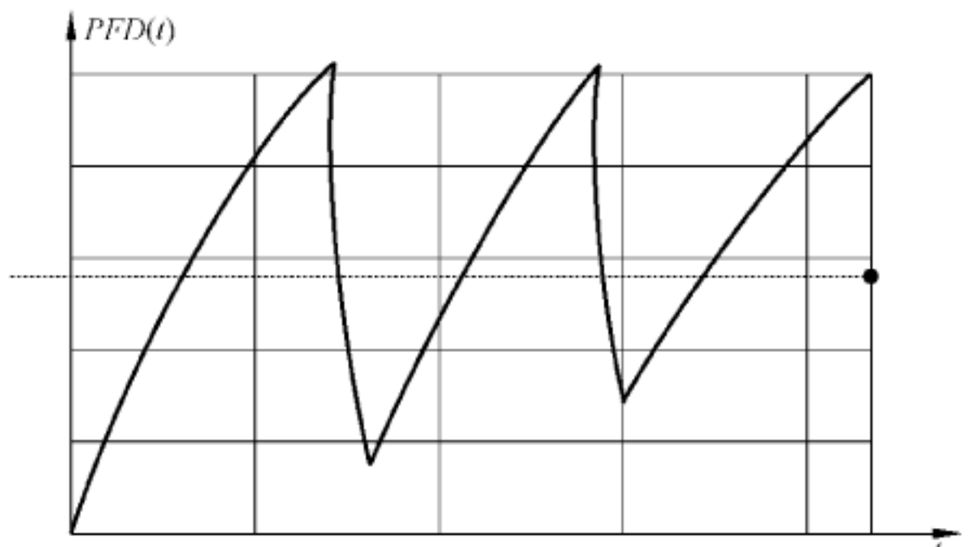


图 B.25　利用多相马尔可夫方法得出的锯齿形曲线

将该公式应用于如图 B.24 所示的模型可得：

$$PFD_{avg}(T)=\frac{1}{T}[MCT_{DU}(T)+MCT_R(T)]$$

如果 EUC 在维修期间关闭，可能会约减为只剩第一项。

图 B.25 中的黑圈表示整个计算过程中锯齿形曲线的 PFD_{avg}。

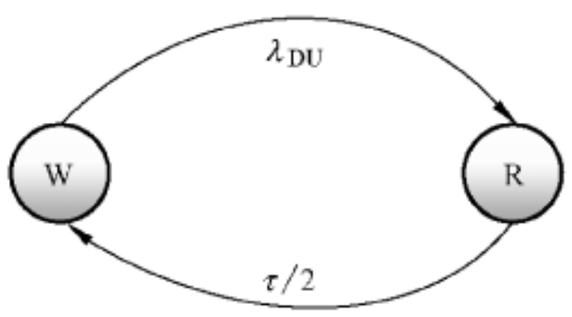


图 B.26　马尔可夫近似模型

注：上述计算通常是基于图 B.26 所示的近似模型，其中状态 DU 和 R 已被合并，$\tau/2$(即，检测失效的平均时间)被用来作为等效修复时间。但这仅适用于通过其他方式已完成马尔可夫方程求解的情况，以便获得这个等效的修复时间。只有在维修时间可以忽略不计情况下这种近似方法才适用。另外，这种方法很难适用于大型复杂系统。

可以很容易地对图 B.24 中的简易模型进行改进，使之可以用于更多实际的部件。如图 B.27 所示，利用连接矩阵对一个拥有两种概率的部件进行建模，其中 γ 表示因测试导致的失效概率(即，真正的要

求时失效),σ 表示(因人为错误导致)测试未能发现的失效概率。

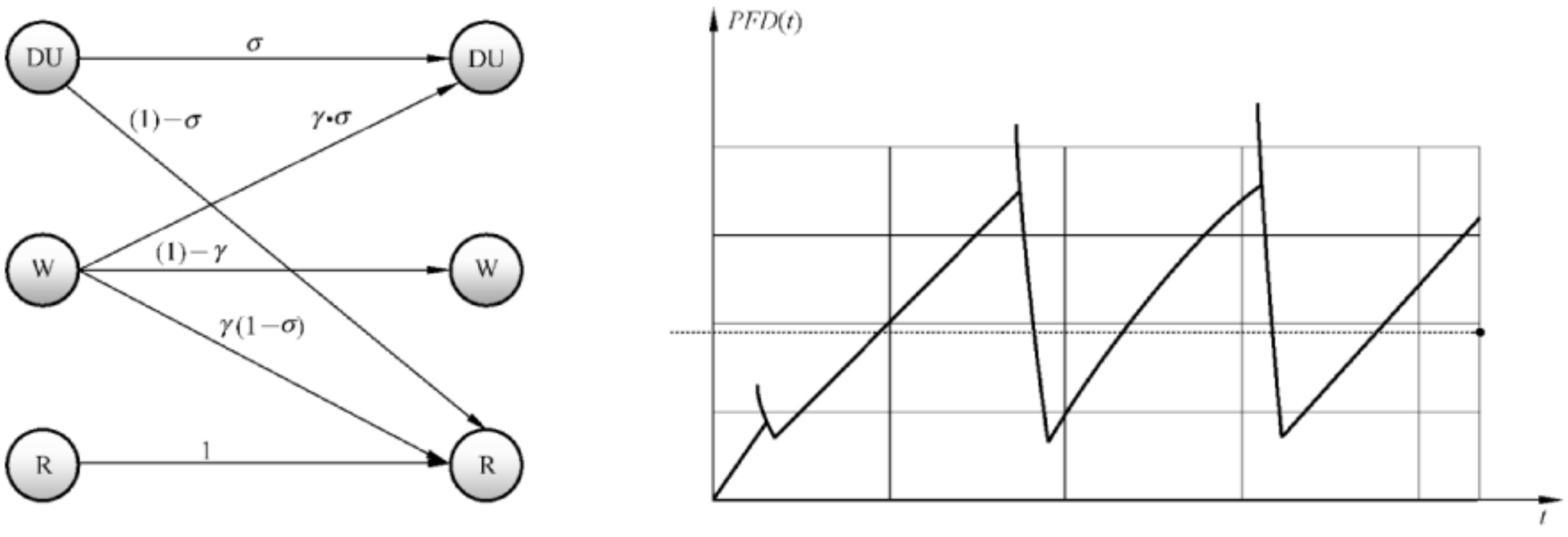


图 B.27　由于要求本身失效的影响

锯齿形曲线的走势发生了变化,各个测试时出现的跳变对应着要求时失效 γ 的概率。同样,黑圈表示 PFD_{avg}。

当一个(冗余)部件在测试中断开时,在整个测试期间它就变为不可用了,这将影响到它的 PFD_{avg}。因此,应当考虑测试时间 π,并在测试间隔内引入一个新阶段,详见图 B.28,在这个阶段中对状态 R 和 W 进行建模,仅是为了实现模型的完整性。

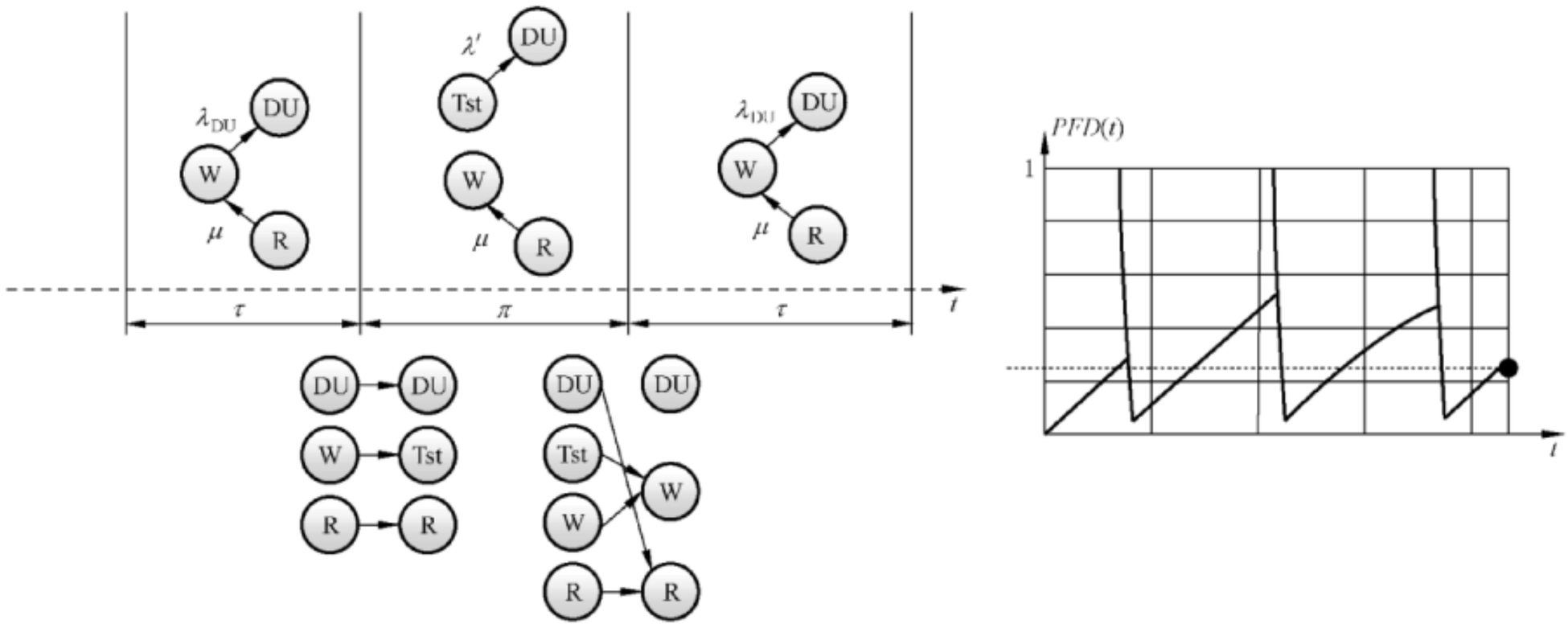


图 B.28　测试时间影响建模

在该马尔可夫模型中,系统在 R、DU 和 Tst 状态下不可用。这种情况比之前更复杂了,但是计算原理仍然一样。锯齿形曲线走势见右图。系统在测试期间内不可用。这是对 PFD_{avg} 最大的影响因素。

在之前的马尔可夫图形中,只考虑了未能检测到的危险失效,但是对可检测的危险失效也可很好地进行建模。区别在于检测到危险失效后立刻开始进行维修(如图 B.29 所示)。因此,当 μ_{DU} 为修复率($\mu_{DU}=1/MRT$)时,μ_{DD} 为部件的恢复率($\mu_{DD}=1/MTTR$)。

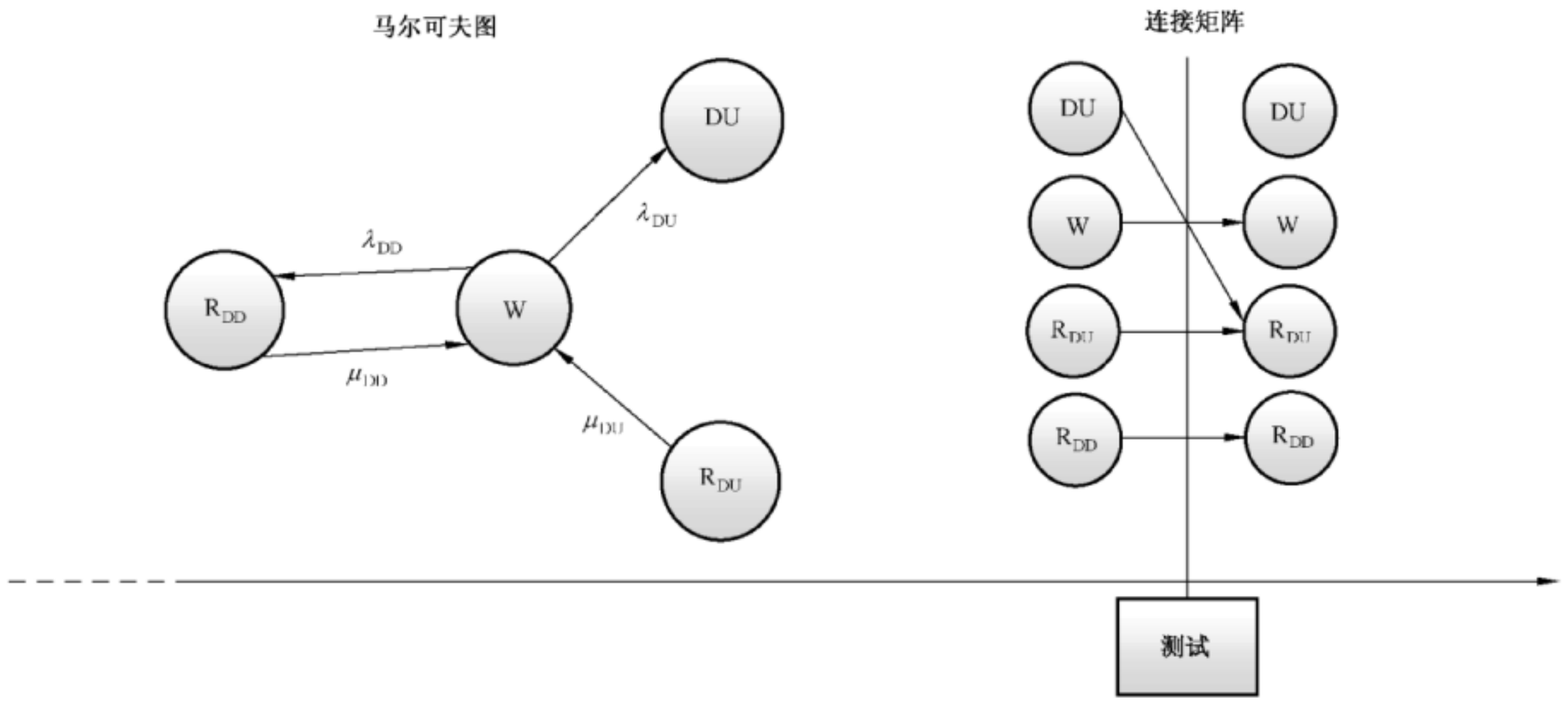


图 B.29　包含 DD 和 DU 失效的多相马尔可夫模型

如果需要，还应当对安全失效进行建模，但此处选择了尽可能简单的马尔可夫图表达。

马尔可夫图法的主要问题是：随着所研究的部件数量增加，状态数量按指数规律增加。如果不进行大量的近似，采用人工进行马尔可夫图建模和计算就会变得非常困难。

使用一个高效的马尔可夫软件包可帮助解决计算上的困难。有大量的软件包可供选用，虽然它们不是专门用于计算 PFD_{avg}，它们大多是用于计算瞬时不可用率，但只有一部分是用于计算状态平均累积时间，而只有极少数能用于多相建模。但无论如何，用它们来计算 PFD_{avg} 并没有什么困难。

就建模本身而言，当部件之间的相关性很弱时，可以综合利用马尔可夫方法和布尔方法：

——马尔可夫模型用于建立各个部件瞬时不可用率；

——通过故障树或可靠性框图，将单个不可用率合在一起计算整个系统瞬时不可用率 $PFD(t)$；

PFD_{avg} 通过对 $PFD(t)$ 进行平均计算得到。

这种混合方法见 B.4，而图 B.25、B.27 和 B.28 所示锯齿形曲线可以作为故障树方法的输入。

当无法忽略部件之间的相关性时，可利用一些工具自动建立马尔可夫图。这些工具是基于比马尔可夫图更高级的模型（如：佩特里（Petri）网和形式化语言）。由于状态数量的组合激增，仍然会导致计算上的困难。

这种组合方法对复杂系统进行建模非常有效。

图 B.30 建模的系统是由三个在同一时间测试且以 2oo3 方式运行的部件构成。检测到失效时，逻辑从 2oo3 变为 1oo2，因为从安全角度来说，1oo2 比 2oo3 更好（但是从误停机失效的角度来说要差）。只有在第二次检测到失效时，才会进行维修，将三个部件都更换成新的部件。这构成了一种系统性约束，从而不可能通过组合部件的独立运行状况来对整个系统的运行状况进行建模。

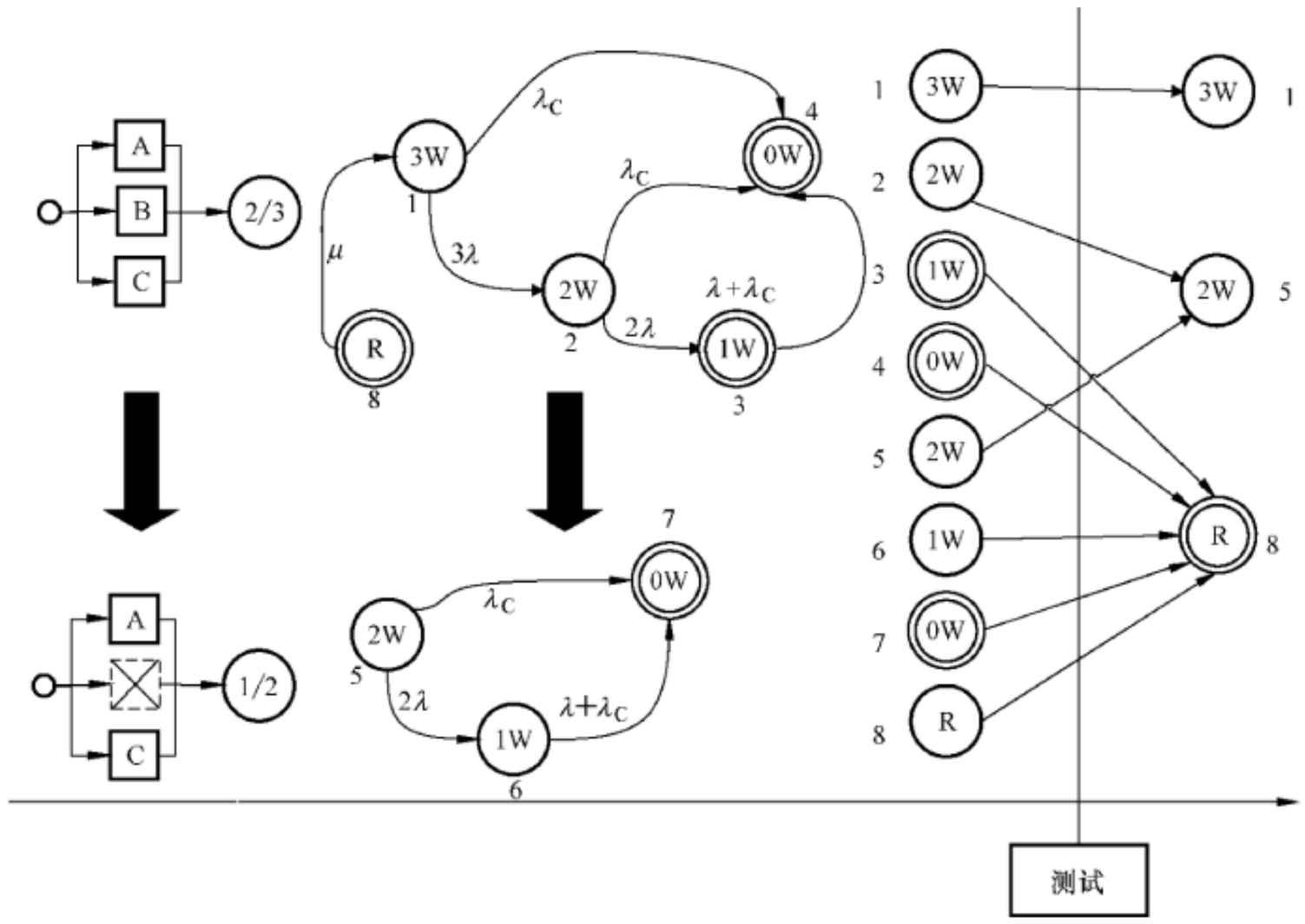


图 B.30　改变逻辑(2oo3 至 1oo2)而不是对首次失效进行维修

B.5.2.2　*PFH* 计算原理

对于 *PFH* 计算,相同类型的多相马尔可夫建模方法可用于对只能通过检验测试检测到的 DU 失效。为了简化,这里只介绍了针对 DD 失效的 *PFH* 计算原理,其仅需要用到常规的(单相)马尔可夫模型。当然,对于处于连续运行模式且只有通过定期检验测试检测的 DU 失效的 E/E/PE 安全相关系统来说,应该使用多相马尔可夫方法。下面介绍的原理仍将适用。

图 B.31 表述了同一个系统的两种马尔可夫模型,这个系统由拥有共因失效的两个冗余部件组成。左图中的部件(A 和 B)是可以维修的,而右图中的部件是无法修复的。

在两个图中,状态 4(AB)是吸收态。发生总体性失效后,系统将保持在失效状态,此时 $P(t)=P_1(t)+P_2(t)+P_3(t)$

为在[0,t]间隔没有发生失效的概率。可知,$R(t)=P(t)$为系统可靠度,而

$F(t)=1-R(t)=P_4(t)$为不可靠度。

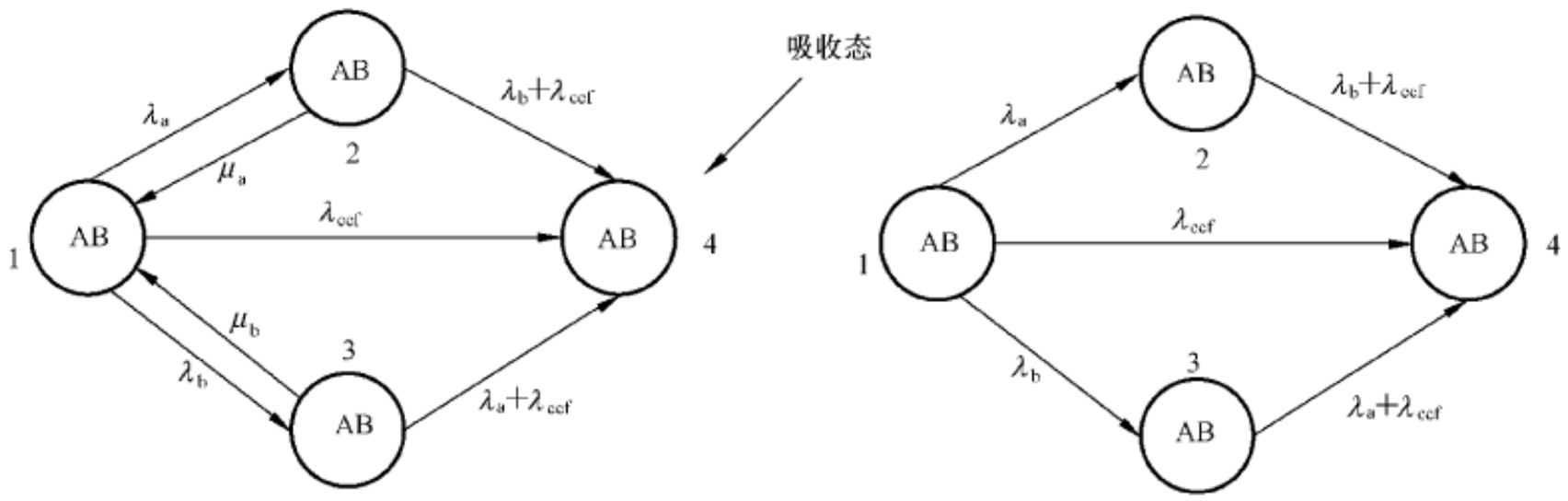


图 B.31　带吸收态的“可靠度”马尔可夫图

如 B.2.3 所述，该可靠性模型适用于 E/E/PE 安全相关系统出现失效并立即引起危险的情况。另外，μ_a 和 μ_b 都表示部件的恢复率(如 $\mu_a=1/MTTR_a$ 和 $\mu_b=1/MTTR_b$)

此类可靠度马尔可夫图可直接通过 $PFH=F(T)/T$ 求得 PFH。例如，在图 B.31 中直接求得 $PFH(T)=P4(T)/T$(假设 $P4(T)<<1$)。

另外，利用该马尔可夫图可用下列公式计算系统 $MTTF$：

$$MTTF=\lim_{t\to\infty}\sum_{k=1}^{n}a_k MCT_k(t)$$

其中，$MCT_k(t)$为状态 K 的平均累积时间；如 k 为良好运行状态，则 $a_k=1$；在其他情况下，$a_k=0$。

上限值为：

$$PFH\approx 1/MTTF$$

几乎所有的马尔可夫软件包都提供有效的算法，可用于计算 $F(T)$和 $MTTF$。

在任何情况下，即使在没有整体系统常数失效率(见图 B.31 右侧图表)的情况下，上述 PFH 预测值仍然有效。唯一的约束就是采用具有一个(或多个)吸收态的马尔可夫可靠性图模型。当然这在使用多相模型时仍然有效。

当所有状态可以快速完全修复时，整体系统失效率 $\Lambda(t)$迅速收敛为一个渐近值 $\Lambda_{as}=1/MTTF$。在该模型图中，除了理想状态和吸收态以外，所有状态都是准瞬时变化的(原因是和 $MTTF$ 相比，部件的 $MTTR$ 是比较短的)。这样就可以直接计算从完好状态到吸收态各种情形的整体系统常数失效率。图 B.31 左侧的马尔可夫图对这样一个可以快速且完全修复的系统进行了建模。即：

——$1\to 4:\Lambda_{14}=\lambda_{ccf}$

——$1\to 2\to 4:\Lambda_{124}=\lambda_a(\lambda_b+\lambda_{ccf})/[(\lambda_b+\lambda_{ccf})+\mu_a]\approx\lambda_a(\lambda_b+\lambda_{ccf})/\mu_a$

——$1\to 3\to 4:\Lambda_{134}=\lambda_b(\lambda_a+\lambda_{ccf})/[(\lambda_a+\lambda_{ccf})+\mu_b]\approx\lambda_b(\lambda_a+\lambda_{ccf})/\mu_b$

在上述 1→3→4 情境的公式的中，λ_b 为从完好状态跳变到其他状态的转移率，$(\lambda_a+\lambda_{ccf})/\mu_b$ 为从状态 3 跳变至状态 4 而不是返回到状态 1 的概率。

最终可得：$\Lambda_{as}=\Lambda_{12}+\Lambda_{124}+\Lambda_{134}=1/MTTF$

这可以简单地推广到复杂的马尔可夫图模型，但是仅适用于快速且完全可修复的系统，即 DD 失效。

图 B.31 右侧马尔可夫图模型不是可快速完全修复的系统。因此应用上述计算方法将得出错误的结果。

当处于连续运行模式的 E/E/PE 安全相关系统和其他安全层共同使用时，应考虑 E/E/PE 安全相关系统的可用度，详见图 B.32 所示两个模型图：此时，不存在吸收态，且在出现整体失效之后系统是可被修复的。$P(t)=P_1(t)+P_2(t)+P_3(t)$为系统在状态 t 时刻正常运行的概率。可知，$A(t)=P(t)$为可用度，$U(t)=1-A(t)=P_4(t)$为不可用度。

这种情况不同于图 B.31 所示，应正确使用 $R(t)$和 $A(t)$，从而获得正确的 $U(T)$和 $F(T)$。

在 DD 失效情况下，处理该问题最简单的方式就是通过 MDT 和 MUT 计算 PFH 的上限值，详见 B.2.3。

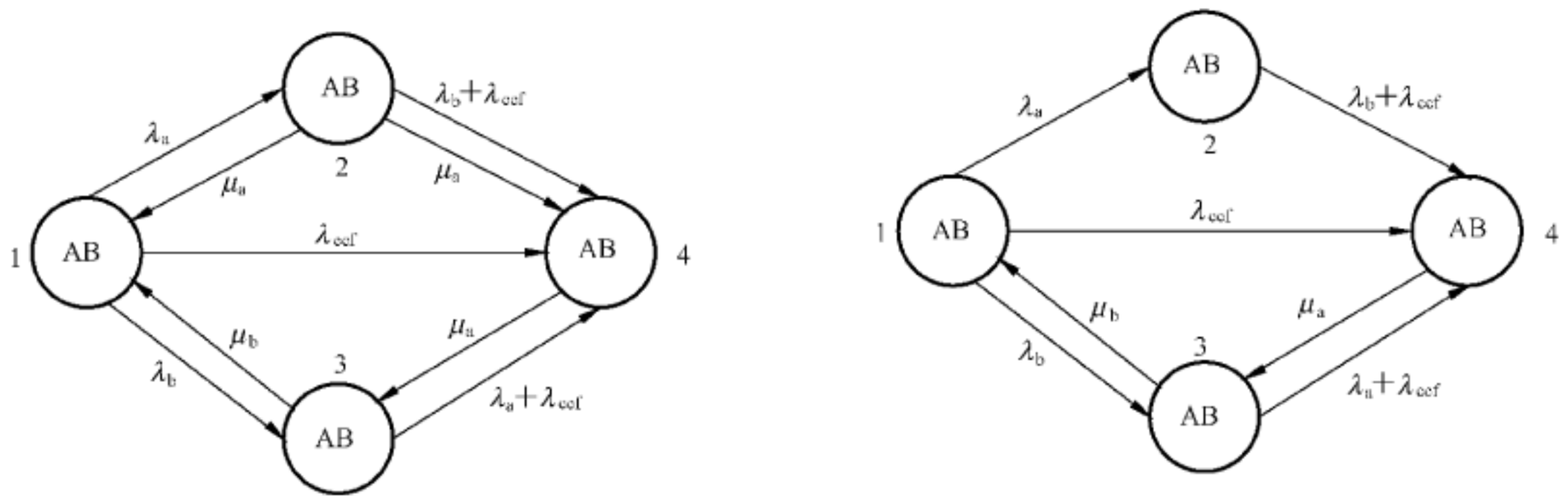


图 B.32　无吸收态的“可用度”马尔可夫图

可用度马尔可夫图的一个有趣特性是：当进入既定状态概率等于离开该状态的概率时，将达到一种渐近平衡。可得：

——$P_{i,as}=\lim_{t\to\infty}P_i(t)$为 $P_i(t)$的渐近值；

——$\lambda_i=\sum_{j\neq i}\lambda_{ij}$为从状态 i 至任何其他状态的转移率。

每一次系统访问状态 i，处于该状态的平均时间为 $Mst_i=1/\lambda_i$

从而可以计算，$MUT=\sum_i(1-q_i)P_{i,as}Mst_i$ 和 $MDT=\sum_i q_iP_{i,as}Mst_i$

其中

如果 i 为运行状态，则 $q_i=0$，在其他状态下，$q_i=1$。

最后可得：$PFH=1/(MUT+MDT)=1/\sum_i P_{i,as}Mst_i=1/\sum_i\frac{P_{i,as}}{\lambda_i}$

注：可以通过 $n=T/\sum_i\frac{P_{i,as}}{\lambda_i}$ 得出[0，T]间隔内的失效次数。

由于大多马尔可夫软件包都能够找到渐近概率，实现上述计算不会特别困难。

当所研究的周期太短，不足以使马尔可夫过程收敛，则计算方法为：$W(t)=\sum_{i\neq f}\lambda_{if}P_i(t)$

可得：$PFH(T)=\sum_{i\neq f}\lambda_{if}\frac{\int_0^T P_i(t)\,dt}{T}=\frac{\sum_{i\neq f}\lambda_{if}MCT_i(T)}{T}$

由于马尔可夫软件包可以给出各个状态的累积时间，进行此类计算也是没有任何问题的。

对于快速可完全修复的系统（DD 失效）来说，维塞利（Vesely）比率 $\Lambda_v(t)$ 快速收敛为一个渐近值 Λ_{as}，这是整体系统常数失效率的一个很好的近似值。因而在这种情况下，可以采用与可靠性计算相同的方式计算 PFH 值。

对于 DU 失效，由于多相建模的缘故，计算较为复杂。上述公式可以演变为：$PFH(T)=\frac{\sum_{\varphi=1}^{n}\sum_{i\neq f}\lambda_g MCT_i(T_\varphi)}{\sum_{\varphi=1}^{n}T_\varphi}$

其中，T_φ 为阶段 φ 的持续时间。

一般情况下，当跳出一种既定状态的概率等于进入该状态的概率时，多相马尔可夫过程将达到平衡状态。此时，渐近值与上述值无关，但可以用于上述公式。

总之，有了马尔可夫方法，就可以通过很多方式计算处于连续运行状态的 E/E/PE 安全相关系统

的 PFH 值。但是仍然需要掌握所依据的数学原理,才能够运用自如。

B.5.3 佩特里(Petri)网和蒙特卡罗模拟法

B.5.3.1 建模原理

对一个动态系统进行有效建模的方法就是建立一种与所研究的 E/E/PE 安全相关系统行为尽可能一样的有限状态自动机。佩特里(Petri)网(见 GB/T 20438.7—2017 的 B.2.3.3 和 B.6.6.10)已被证实能非常有效地实现这一目的,原因如下:

——可以很容易地以图形方式进行表示;

——模型规模随着建模部件数量的增加而线性增加;

——佩特里网非常灵活,几乎可以对所有的约束条件进行建模;

——可以很好地支持蒙特卡罗模拟(见 GB/T 20438.7—2017 的 B.6.6.8)。

最初为了对自动状态机进行形式上的验证,人们在 20 世纪 60 年代提出了佩特里网,随后其被可靠性工程师分为两个应用领域,第一个是在 70 年代用于自动构造大型马尔科夫图,第二个是在 80 年代用于进行蒙特卡罗模拟。

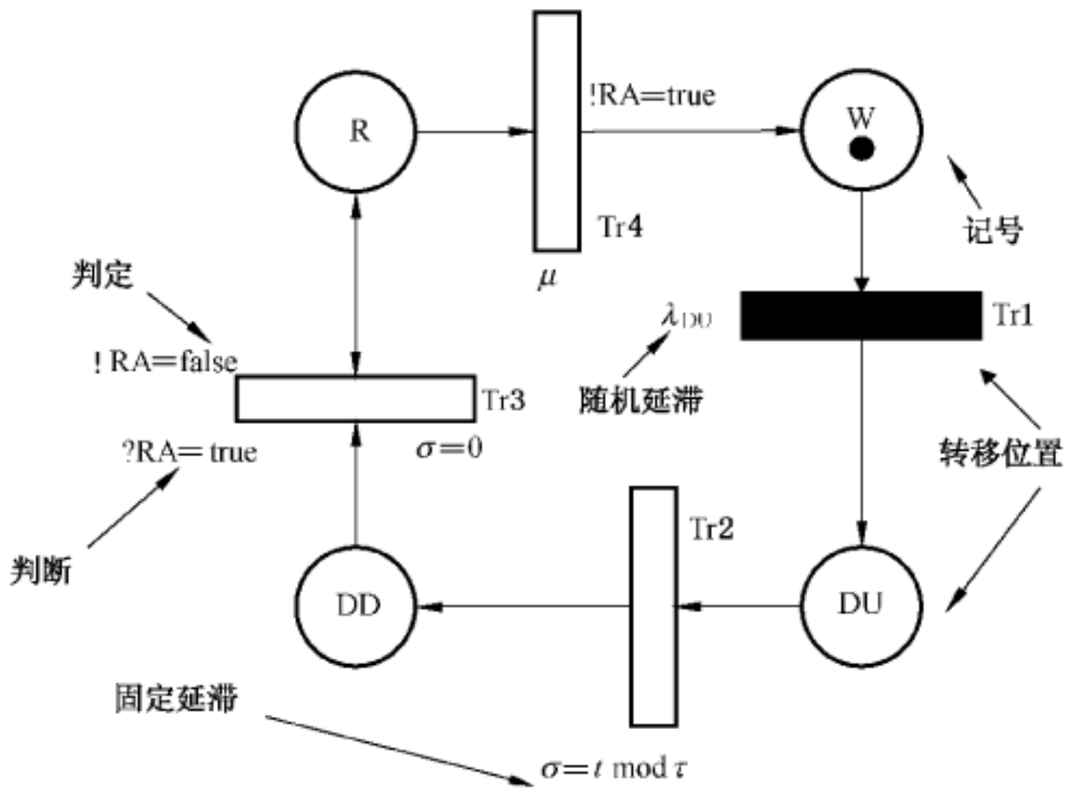


图 B.33 单个周期性测试部件的佩特里网模型

一个简单的单个周期性测试部件的典型子佩特里网模型由三个部分构成:

1) 静态部分(即所绘制的图形):
   a) 与潜在状态相应的库所(圆圈);
   b) 与潜在事件相应的转移(矩形);
   c) 确认转移的上游箭头(从库所到转移);
   d) 表示转移触发的下游箭头(从转移到库所)。
2) 时序部分:
   a) 随机迟延,表示事件发生前的随机延迟时间;
   b) 固定迟延,表示事件发生前的确定延迟时间。
3) 动态部分:
   a) 事件发生时令牌(小黑圈)移动,表示实际达到的潜在状态;
   b) 确认是否发生转移的预计(结果为真或假的任意公式);
   c) 当触发一个转移时对某些变量进行更新的断言(任何方程式)。

此外,一些规则也可以确认和触发转移:

4) 确认出现转移(即:相应事件可能发生的条件):

a) 所有上游库所至少有一个令牌;

b) 所有预计的结果必须为“真”。

5) 触发一个转移(即:出现相应事件时可能发生什么情况):

a) 从上游库所去除一个令牌;

b) 从下游库所增加一个令牌;

c) 更新断言。

上面介绍了与佩特里(Petri)网相关的大部分概念,剩余的将在使用时进行介绍。

B.5.3.2 蒙特卡罗模拟原理

蒙特卡罗模拟由多个行为模型的动画构成,通过随机数评估系统处于由随机延迟或固定延迟决定的状态的时间(见 GB/T 20438.7—2017 的 B.6.6.8)。

这可以通过图 B.33 所示佩特里(Petri)网解释:

——最初,令牌处于 W 位置,部件处于良好运行状态。

——在这种状态下只可能发生一种事件——未检测到的危险失效-(转移 Tr1 有效,涂黑)。

——处于该状态的时间为随机的,且服从参数为 λ_{DU} 的指数分布。蒙特卡罗模拟指在发生失效之前(即 Tr1 即将触发)利用一个随机数(见下文)计算延迟 d_1。

——经过 d_1 延迟后,Tr1 被触发,令牌移动至 DU 位置(更确切地说,应该是从 W 位置去除一个令牌,在 DU 位置添加一个令牌)

——部件达到未检测到的危险状态且转移 Tr2 有效。

——发生确定延迟 d_2(其中,$d_2=t$ 按 τ 取模,t 为当前时间,τ 为测试间隔)之后检测到危险失效。这对测试间隔进行了模拟。

——经过 t_2 后,危险失效被检测到,令牌进入 DD 位置。此时部件等待维修,Tr3 变为有效。

——触发 Tr3(开始维护)的延迟 d_3 不由部件本身决定,而是取决于由信息 RA 所代表的维修资源的可利用性。这受整个佩特里网模型的另一部分中的事件的控制,其未在图 B.33 中进行表示。

——一旦维修团队可以服务,就开始进行维修(即:预计?RA =true 结果为真),这时令牌进入库所 R。对于其他的中断请求,维修资源立刻变为不可用,并且通过断言! RA=false 来更新 RA 值,以防止在同一时间进行其他的维修操作。

——随机转移 Tr4(即维修过程结束)变为有效,可以利用一个基于修复率 μ 的随机数来计算延迟 d_4。

——经过 d_4 延迟后,Tr4 状况被触发,部件恢复到良好运行状态(令牌进入 W 位置)。通过断言! RA=true 更新 RA,使得维修资源再次变为可用。

——重复上述过程... 只要在[0,T]间隔内有下一个有效转移状态发生。

当下一次转移不在[0,T]间隔内,模拟将被停止,从而形成部件的一条历史记录。在整个历史进程中,可以对相关参数进行记录,如库所的平均标记(即:在 T 持续时间内一个令牌处于一定库所的时间比)、转移触发的频率、既定事件第一次发生的时间等。

蒙特卡罗模拟原理的作用是可以获得大量的历史记录,并对相关结果进行经典的统计分析,以便评估相关参数。

与解析计算相反,通过蒙特卡罗模拟,可以轻易将固定延迟和随机延迟混合在一起,随机延迟可以通过累积概率分布 $F(d)$ 和在[0,1]间隔内均匀分布的随机数 Z_i 模拟获得。几乎所有的编程语言都支持这些随机数,并可利用很多的有效算法来实现。

然后根据 $d_i=F^{-1}(z_i)$,可以通过 Z_i 求得按 $F(d)$ 分布的样本集(d_i)。当可以得到 $F^{-1}(z)$ 的解析

形式时，这个过程就变得非常简单。例如，呈指数分布的延迟：$d_i = -\frac{1}{\lambda_{DU}}\mathrm{Log}(z_i)$。

考虑到计算的准确性，给定一个模拟参数 X，利用模拟的样本集(X_i)，通过基本统计原理可以计算样本的平均值、方差、标准差和置信区间：

——平均值：$\overline{X} = \frac{\sum_i X_i}{N}$；

——方差：$\sigma^2 = \frac{\sum_i (x_i - \overline{X})^2}{N}$，标准差：$\sigma$；

——$\overline{X}$ 周围 90%的置信区间：$Conf = 1.64\frac{\sigma}{\sqrt{N}}$

由此，使用蒙特卡罗模拟时，总是可以预测到结果的精度。例如，真实结果 $\hat{X}$ 属于间隔 $[\overline{X} - 1.64\sigma/\sqrt{N}, \overline{X} + 1.64\sigma/\sqrt{N}]$范围内的几率为 90%。

当历史记录数量增加以及 X 出现频率增加时，该区间将变小。

利用当前的个人计算机，即使对 SIL4 的 E/E/PE 安全相关系统的计算也不会存在实际的困难。

B.5.3.3 *PFD* 计算原理

由于 W 位置的平均标记就等于持续时间 T 内 W 位置的时间比(即 W 位置被令牌标记)，这实际上就是部件的平均可用率 A。图 B.33 所示子佩特里网可直接用于计算部件的 PFD_{avg}。由此可得：$PFD_{avg} = 1 - A$

依据上面所述，也可以估算这种计算方法的精度。

通过特定的子 Petri 网可以表示更加复杂的运行状况。图 B.34 对周期性测试部件、共因失效(CCF)和维修资源的建模，给出了示例。

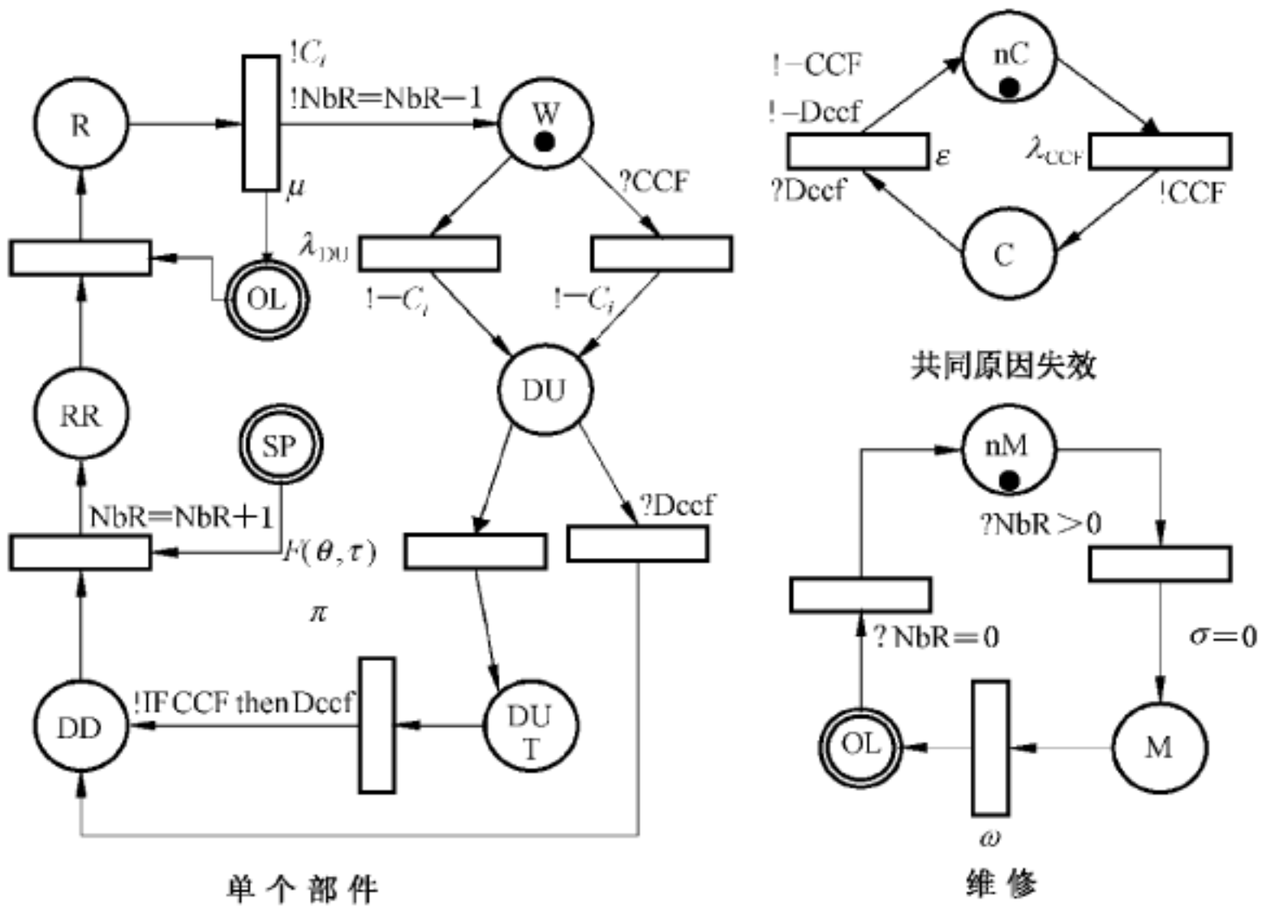


图 B.34 佩特里网建模共因失效和维修资源

左侧显示了一个周期性测试部件的模型，该部件在正在运行(W)、未检测到危险失效(DU)、正在测试(DUT)、检测到危险失效(DD)、准备进行维修(RR)以及正在维修中(R)等状态间跳转。

出现失效时(DU)，系统将发出！$-C_i$(等同于！C_i = false)通知部件出现失效。然后等待启动一个周期性测试(DUT)。周期性测试的间隔为 τ、波动时间为 θ。当执行完时长为 π 的测试之后，达到状

态 DD。如果备品备件可用(在 SP 中至少有一个令牌),部件可以准备进行维修(RR),同时变量 *NbR* 增加 1,通知维修资源需要维护的部件数量。当维修资源就位(在 OL 处做一个令牌),就开始维修(R),然后将令牌从 OL 处移除。顺利完成维修后,部件恢复至良好运行状态,这时系统发出! C_i 信息(如! C_i = true),变量 *NbR* 减少 1,将令牌放回 OL 处,允许进行下一次维修。以此类推。

维修的子佩特里网模型用到了变量 NbR。当该变量为正数时,开始调度维修资源(M),在延迟一定时间后,这些维修资源做好现场工作准备(OL)。OL 处令牌表示开始维修发生失效的部件。因此,同一时间只能进行一个维修动作。当所有维修工作完成后(即,NbR=0),就释放维修资源。

图 B.34 也对一个共因失效(CCF)进行了建模。当出现(λ_{pcc})情况,消息! CCF 变为真,并通过这个消息将所有受影响的部件设置成 DU 状态。与之相关的消息 C_i 变为假,各个部件被单独进行维修。当完成部件测试之后,断言! IF CCF then Dccf 向所有其他部件发出通知:已检测到一个 CCF。该消息用于将这些部件立即设成进入 DD 状态。另外还通过该消息重设 CCF 子佩特里网,但是须在一定时间(ε)之后才能重设,以确保重设之前所有部件都已进入 DD 状态。

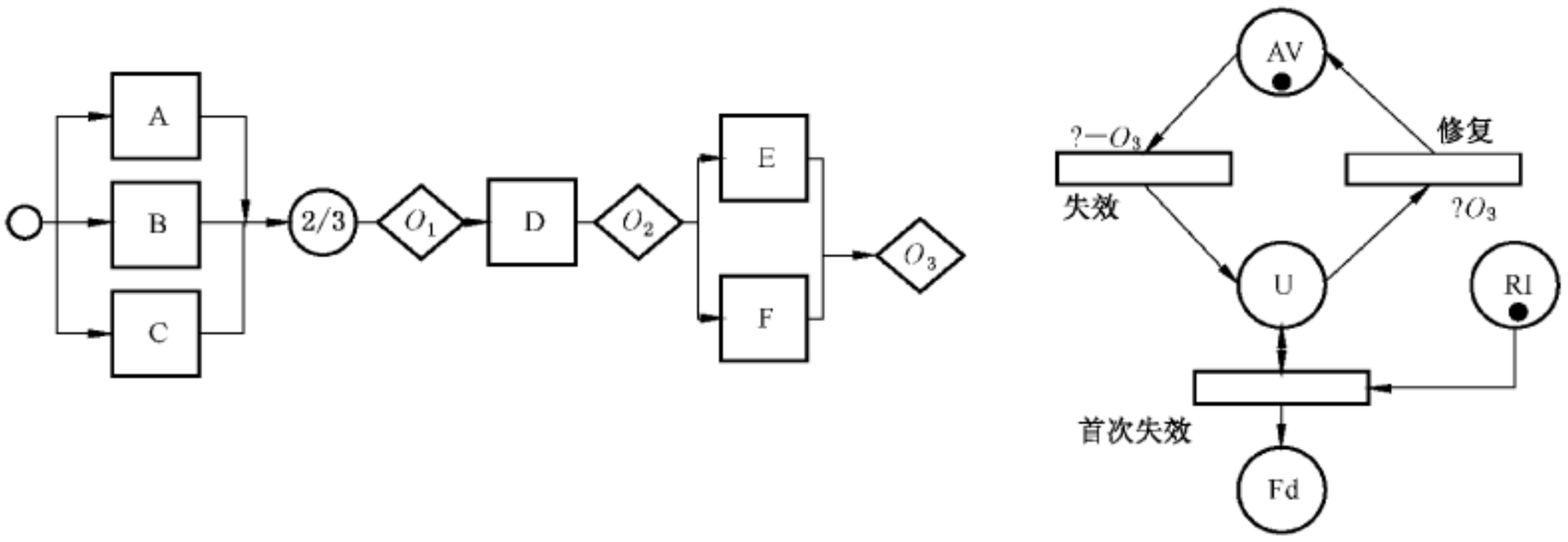


图 B.35　使用可靠性框图构建佩特里网和辅助佩特里(Petri)网用于 *PFD* 和 *PFH* 计算

在图 B.34 中,子佩特里(sub-Petri)网被用作于更复杂模型的一部分。图 B.35 表示了如何使用它们的一种方法,其通过引入中间输出 O_i 对 B.16 中可靠性框图做了轻微的调整。

部件 A、B、C、D、E 及 F 可以通过一系列如图 B.34 所示的子佩特里(sub－Petri)网进行建模,包含部件(A、B、C)的 CCF,用于部件(E、F)的另一个 CCF,所有部件共享同一个维修资源。剩下的问题就是根据可靠性框图逻辑将部件连接在一起,并计算相关 PFD_{avg}。

利用消息 C_i 可以很容易将部件连接在一起,并建立下列断言:

——$O_1 = C_a . C_b + C_a . C_c + C_b . C_c$

——$O_2 = O_1 . C_b$

——$O_3 = O_2 . (C_c + C_f)$

这样,当 O_3 为真时,整个 E/E/PE 安全相关系统运行正常,否则其为不可用。该消息在右侧的子佩特里(sub－Petri)网中,用于对 E/E/PE 安全相关系统的各种状态进行建模:可用(Av)、不可用(U)、可靠(RI)及不可靠(Fd)等。

对于 *PFD* 计算,主要在于 Av 和 U:当 O_3 为假时,系统出现失效并且不可用,当 O_3 为真时,系统恢复并再次可用。可以很容易地得出,Av 的平均标记为系统的平均可用率,而 *U* 的平均标记为平均不可用率,即 PFD_{avg}。

因而,蒙特卡罗模拟可以自动进行瞬时不可用率积分,除非需要得到锯齿形曲线,否则无需计算瞬时不可用率。它可以通过对在给定的瞬时时间而不是整个[0,T]间隔内 *U* 的平均标记来轻易地求得。

上述内容说明了佩特里网可以广泛地用于 *SIL* 计算,但事实上,可以用其进行建模的潜在应用领域还远远不止这些。

B.5.3.4 *PFH* 计算原理

PFH 计算原理和上文一样，也使用与 DU 失效相同的子模型。图 B.36 展示了一个对 DD 失效进行建模的子佩特里网，该失效一旦被检测后将立即暴露出来并被修复。

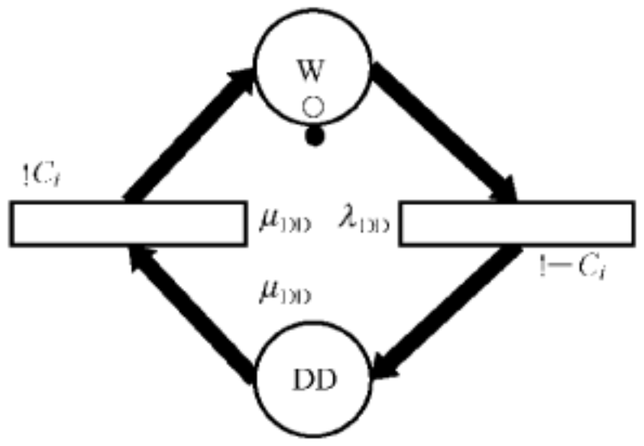


图 B.36 出现失效和修复的单部件的简易的佩特里网模型

如前所述，该部件模型可用于建立如图 B.35 所示的整个系统可靠性框图间的关系。

当处于连续运行模式中的 E/E/PE 安全相关系统是最终安全层时，一旦发生失效将会出现意外事件，因而必须通过系统可靠性进行 *PFH* 求值。详见图 B.35 右侧子 PN 下半部分：系统在[0，*T*]间隔内首次失效平均频率等同于其不可靠度 $F(T)$。然后当 $F(T)$远小于 1 时，根据 *PFH* 定义，可知 $PFH = F(T)/T$。

由于令牌处于 RI 处，首次失效为一次转移。假设所有历史记录均指向一个失效(即 T 足够长)，那么令牌处于 RI 处的平均时间就等于系统 *MTTF*，$PFH \approx 1/MTTF$ 即为 *PFH* 上限值。

当处于连续运行状态的 E/E/PE 安全相关系统不是最终安全层时，在出现失效时不会直接导致意外事件。这样的话维修发生在出现整体失效之后，并应通过系统不可用度计算 *PFH* 值。这可以直接通过转移失效的频率 *Nbf* 求得。从而获知系统在给定时期内出现失效的次数。由此可得：$PFH(T) = Nbf/T$

有趣的是当 *T* 足够长时，可以通过状态 Av 的平均累积时间 MCT_{Av} 计算 *MUT*，以及通过状态 *U* 的平均累积时间 MCT_U 计算 *MDT*。在蒙特卡罗模拟中，通过对令牌处于 Av 和 U 处的累积时间可以很容易地计算出平均累积时间 MCT_A 和 MCT_U。可知：$MUT = MCT_A/Nbf$ 和 $MUT = MCT_U/Nbf$。这可以用于以下求值：$PFH = 1/(MUT + MDT) = 1/MTBF = Nbf/T$。

由于蒙特卡罗模拟可以很自然地给出平均值，所有这些结果都可以直接求得。上述内容说明了佩特里网可以广泛地用于 SIL 计算，但事实上，可以用其进行建模的潜在应用领域还远远不止这些。

B.5.4 其他方法

模型的规模和所研究的系统部件数量间的关系随着使用方法的不同会发生巨大变化。对于故障树和佩特里网来说，其关系为线性；但是对于马尔可夫过程来说，其关系为指数性。所以和马尔可夫方法相比，故障树和佩特里网方法更便于处理大型系统。这就是为什么有时候通过佩特里网来生成大型马尔可夫图。

下面所述的在图形方法之后的形式化语言描述了上述产品的平面模型：各部件都在同一层次上，被单独建模。这使得大型模型在有的时候较难处理和维护。克服该问题的方法就是通过结构化语言建造分层的紧凑模型。最近已提出了多个这样的形式化语言，也有一些软件包可以应用。例如，我们可能会想到 2000 年出版的 AltaRica 数据流语言，可以由可靠性专业人员自由使用，其设计目的是准确地对工业系统的功能和功能障碍特性进行建模(参见 B.7 中的内容)。

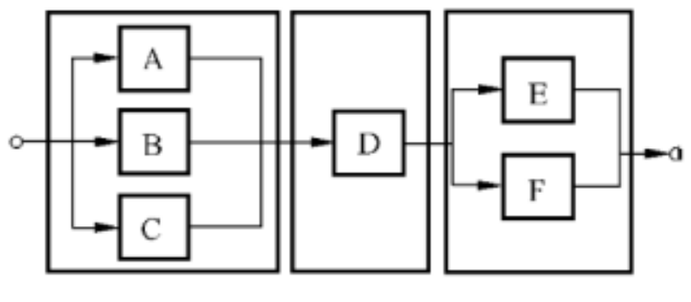
图 B.37 等同于图 B.1 所示可靠性框图。该模型为分层模型，对单个模块只需建一次模型，然后根据需要可以在系统层次上重复多次使用(即，在主节点中)。这样就可以实现非常紧凑的模型。

为了简化描述，只描述了部件的两个转移状态：失效和维修（即：一旦出现 DD 失效，就立即暴露出来，并进行维修）。

通过逻辑算符（or，and）描述系统逻辑。这可以通过可靠性框图与流程 Out 间的直接关系对系统状态进行建模：当 Out 为真时，系统运行正常；当 Out 为假时，系统失效。

```
node bloc
   atate working:bool;
   flow input:bool:in; output:bool:Out;
   event failure, repair;
   init
      working:=true;
   trans
      working       | - failure -> working:=flase;
      not working  | - repair  -> working:=true;
   assert
      output = if working then input else false;
   extern
      law <event failure> = exponential (lambda);
      law <event repair>  = exponential(mu);
      parameter lambda = 1e-3;
      parameter mu       = 0.01;
edon

node main
   sub A:bloc; B:bloc;
         C:bloc; D:bloc;
         D:bloc; E:bloc;
   assert
      A. input = true, B.input = true,  C.input = true,
      D. input = (A.output or B.output  or C.output),
      E. input = D.output,
      F. input = D.output;
      out       = (E.output or F.output)
   extern
      predicate failed = <term (not Out)>;
      locker     failed = <term (not Out)>;
edon
```



单模块

可靠性数据

系统

意外事件

图 B.37　通过形式化语言进行功能和功能障碍建模示例

这可以为有效地运用蒙特卡罗模拟方法提供很好的行为模型，且对于 PFD_{avg} 和 PFH 的计算来说，上面介绍的所有与佩特里网相关的内容仍然适用。因而在此不进一步探讨。

该形式化语言具备与佩特里网类似的数学属性，因而可以很容易地将一个模型编译成为另一个模型。这同时也可以推广适用到故障树或马尔可夫过程所依据的语言属性。因此，假设相关描述仅限于马尔可夫过程或故障树属性，则有可能将模型编译为对等的马尔可夫图或故障树。模型后半部分的关键词“predicate”和“locker”的目的就是提供生成故障树或马尔可夫模型的指令或直接进行蒙特卡罗模拟的指令。

从功能和功能障碍角度说，使用专门设计的对系统行为进行建模的形式化语言使得：

——可以直接在模型上进行蒙特卡罗模拟；

——按照前文所述要求生成马尔可夫图和进行解析计算（当语言限制于马尔可夫属性时）；

——按照前文所述要求生成同等的故障树和进行解析计算（当语言限制于布尔属性时）。

此类用于描述功能和功能障碍的形式化语言都是通用语言。用于 E/E/PE 安全相关系统这一特定应用时不会有任何困难。当存在多个保护层、多种类型失效模式、复杂的检验测试模式、部件间存在相关性、维修资源等，即当其他方法已经难以处理时，这些语言可以为实现一个 E/E/PE 安全相关系统的 PFD_{avg} 和 PFH 的计算提供非常有效的方法。

B.6 处理不确定性

进行概率计算时，面临的一个主要问题是可靠性参数的不确定性。因而，在进行 PFD 和 PFH 计算时，对结果不确定性的影响进行评估，是很有帮助的。

处理此类问题需要很仔细，而蒙特卡罗模拟是实现这一目的一种有效方法，详见图 B.38。

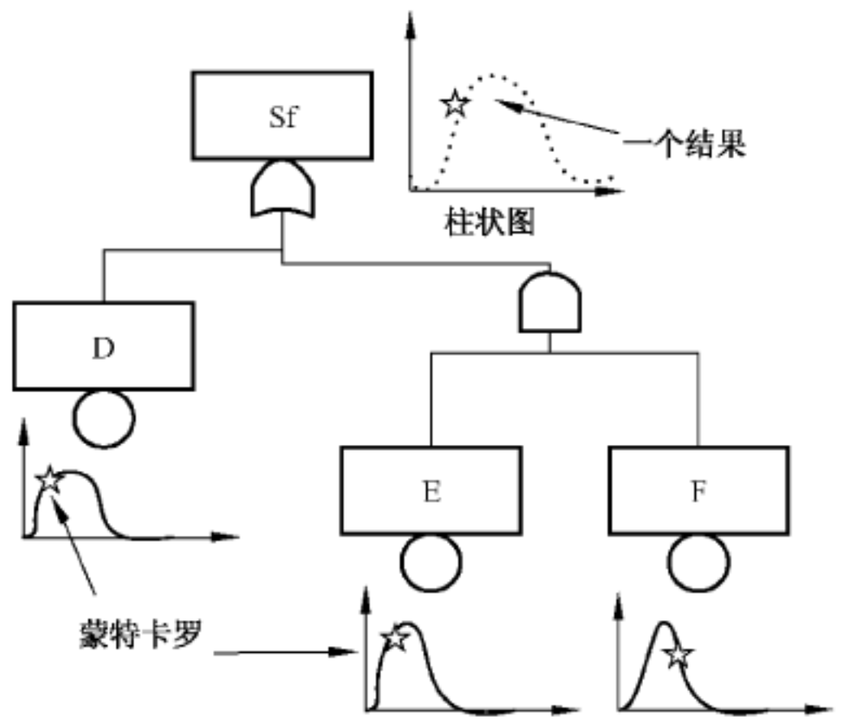


图 B.38 不确定性传递原理

如图 B.38 所示，输入的可靠性参数(即未检测到的危险失效率)不再是确定数值，他们被随机变量所替代。根据不确定性的程度不同，此类随机变量的概率密度的变化或多或少，或突变或平坦：F 的概率密度比 E 或 D 的更陡峭。这意味着 F 的不确定性比 E 或 D 的不确定性更少些。

计算原理如下：

1) 根据这些参数的概率分布通过随机数生成一套输入参数(和 B.3.2 解释类似)；
2) 通过上述生成的输入参数进行计算；
3) 记录输出结果(得出第 4 步需要使用的一个数值)；
4) 在获得足量数值(如 100 或 1 000)之前，重复进行第 1 步～第 3 步，最终可以形成一个柱状图(如图 B.38 中的虚线)，；
5) 统计分析柱状图，求得平均值和输出结果的标准差。

根据计算类型，柱状图平均值可能是 PFD_{avg} 或 PFH，而通过标准差可以估量结果的不确定性。标准差越小，PFD_{avg} 或 PFH 计算值越准确。

这里介绍的故障树原理较为通用，可以应用于本附录中的任何计算方法：简化公式、马尔可夫过程及佩特里网或形式化语言方法等。当已经通过蒙特卡罗模拟进行计算之后，应当采用一种两步骤的蒙特卡罗模拟。

应根据相关知识选择既定可靠性输入参数的概率分布，可以是：

——在上限值和下限值之间的均匀分布；

——最可能值的三角形分布；

——给定误差因子的对数常态法则；

——卡方法则等。

当只有少量现场反馈时，可以通过工程判断评估前半部分分布。当拥有大量现场反馈时，可以使用后半部分分布，这是因为现场反馈可以提供平均参数值和这些平均值的置信区间。

例如，如果在累积观测时间 T 内观察到 n 个失效，可知：

——$\hat{\lambda}=n/T$ 为失效率的最大似然估计量；

——$\lambda_{\inf,\alpha}=\frac{1}{2T}\chi^2_{(1-\alpha),2n}$ 下限值，概率为 α%，低于 $\lambda_{\inf,\alpha}$；

——$\lambda_{\mathrm{Sup},\alpha}=\frac{1}{2T}\chi^2_{\alpha,2(n+1)}$ 上限值，概率为 α%，高于 $\lambda_{\mathrm{Sup},\alpha}$。

当 $\alpha=5\%$，那么 λ 实际值有 90%机会在$[\lambda_{\inf,\alpha},\lambda_{\mathrm{Sup},\alpha}]$间隔内。该间隔越小，$\lambda$ 值越准确。一般情况下，好的可靠性数据库可以提供这些信息。分析人员应当谨慎考虑没有置信区间(或可用于对其进行计算的信息)的可靠性数据。

$\hat{\lambda}$，$\lambda_{\inf,\alpha}$ 和 $\lambda_{\mathrm{Sup},\alpha}$ 都可以用于建立相关的分布，以对给定失效模式的失效率 λ 和不确定性进行建模。对于 χ^2 分布来说，这是比较明显的，但是，对于对数常态法则分布，也表明这是非常有效的。这种对数常态法则分布由平均值 $\hat{\lambda}$ 或其中值 $\lambda_{50\%}$ 以及所谓的误差因子进行描述。

该法则有一个很有趣的属性：$\lambda_{\inf,\alpha}=\lambda_{50\%}/ef_\alpha$ and $\lambda_{\mathrm{Sup},\alpha}=\lambda_{50\%}\cdot ef_\alpha$。

这样，其仅需要通过两个参数就可定义：λ and $ef_\alpha\approx\sqrt{\frac{\lambda_{\mathrm{Sup},\alpha}}{\lambda_{\inf,\alpha}}}$

当 $ef_\alpha=1$，就不存在不确定性，当 $ef_\alpha=3.3$，在置信区间的上下边界值之间存在一个约为 10 的因子，等等。

这些分布随后可以用于蒙特卡罗模拟，以便同时考虑平均值和不确定性对 PFD_{avg} 和 PFH 的影响。因而总是可以通过概率计算的范围来控制不确定性。一些软件包可以直接进行此类计算。

在进行冗余系统分析时，不仅需要考虑基本元件失效率的不确定性，还要考虑 CCF 失效率的精度。尽管对于各个元件有较好的现场反馈数据，但是很少有好的 CCF 现场数据，因而其不确定性较大。

B.7 参考

更多有关计算失效概率的信息，请见参考文献[4]～[9]和[22]～[24]。

附 录 C
（资料性附录）
诊断覆盖率和安全失效分数的计算

GB/T 20438.2—2017 附录 C 给出了诊断覆盖率和安全失效分数的计算方法。本附录简要介绍应用该方法计算诊断覆盖率。本文假定 GB/T 20438.2 规定的所有信息均可获得，并用于表 C.1 求值。表 C.2 给出 E/E/PE 安全相关组件要求的诊断覆盖率限制因素。表 C.2 数据来源于工程判断。

为了理解表 C.1 数值，需要一份详细的硬件原理图，通过它可以确定所有失效模式的影响。这些数值仅为示例，例如在表 C.1 中假设一些元器件无诊断覆盖率，是因为实际上不可能检测到所有元器件的所有失效模式。

从表 C.1 可知：

a) 通过失效模式和影响分析，确定每个元器件的各种失效模式在无诊断测试时对系统行为的影响。对于每个元器件，各种失效模式按安全(S)和危险(D)失效划分为相关整体失效率的分数。简单元器件的安全和危险失效划分是可以确定的，但需基于工程判断。对于复杂元器件，不可能对每一个失效模式进行详细分析，所以普遍接受的做法是将失效分为 50%安全和 50%危险。该表使用了参考文献 a)所述的失效模式，尽管也许还有其他的、甚至更好的失效模式划分。

b) 表中给出了各个元器件诊断测试的诊断覆盖率(见"DC_{comp}"列)。给出了检测安全和危险失效具体的诊断覆盖率。尽管简单元器件(如电阻、电容和晶体管)开路或短路失效均可以检测，其具体诊断覆盖率为 100%，表 C.2 中还限制了 U16(一种复杂 B 类元器件)的诊断覆盖率为 90%。

c) 列(1)和列(2)给出了各个元器件在无诊断测试的情况下的安全和危险失效率(分别为 λ_S 和 $\lambda_{DD}+\lambda_{Du}$)。

d) 我们可以将一个已检测的危险失效视为实际的安全失效，因而我们可以将失效划分为实际的安全失效(如已检测的安全失效、未检测的安全失效或已检测的危险失效)和未检测的危险失效。危险失效率乘以危险失效对应具体的诊断覆盖率，将结果与安全失效率[见列(3)]相加，就可以得出实际的安全失效率。同样，用 1 减去危险失效对应具体的诊断覆盖率，并将结果乘以危险失效率[见列(4)]，就可以得出未检测的危险失效率。

e) 列(5)给出已检测的安全失效率，列(6)给出已检测的危险失效率，其分别可以通过将具体诊断覆盖率乘以安全或危险失效率得出。

f) 从表中可得：

——总安全失效率 $\sum\lambda_S+\sum\lambda_{Dd}=9.9\times10^{-7}$

——(包括已检测的危险失效)

——总未检测的危险失效率 $\sum\lambda_{Du}=5.1\times10^{-8}$

——总失效率 $\sum\lambda_S+\sum\lambda_{Dd}+\sum\lambda_{Du}=1.0\times10^{-6}$

——总未检测的安全失效率 $\sum\lambda_{Su}=2.7\times10^{-8}$

——安全失效诊断覆盖率 $\dfrac{\sum\lambda_{Sd}}{\sum\lambda_S}=\dfrac{3.38}{3.65}=93\%$

——危险失效诊断覆盖率

$$\frac{\sum\lambda_{Dd}}{\sum\lambda_{Dd}+\sum\lambda_{Du}}=\frac{6.21}{6.72}=92\%$$

（一般简称为“诊断覆盖率”）

——安全失效分数$\frac{\sum\lambda_S+\sum\lambda_{Dd}}{\sum\lambda_S+\sum\lambda_{Dd}+\sum\lambda_{Du}}=\frac{986}{365+672}=95\%$

无诊断测试的失效率划分：35%安全失效和65%危险失效。

表 C.1　诊断覆盖率和安全失效分数的计算范例

项目	数量	类型	各种失效模式下安全和危险失效的划分										根据诊断覆盖率和计算的失效率划分安全和危险失效(10^{-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	印制电路板	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	OSC24 MHz	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	MC68000－12	0	1	0	1	0.5	0.5	0.5	0.5	0.90	0.90	260.4	483.6	685.6	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：没有对项R6的失效模式进行任何检测，但失效既不会影响安全也不会影响可用性。

说明

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}　　对于元器件特定的诊断覆盖率

参见表B.1，表中仅给出了所讨论的单个元器件的失效率，而不是一个通道中所有元器件的失效率。

表 C.2　不同组件的诊断覆盖率和有效性

元器件	低诊断覆盖率	中诊断覆盖率	高诊断覆盖率
CPU(见注 3)	合计小于 70%	合计小于 90%	
寄存器,内部 RAM	50%～70%	85%～90%	99%～99.99%
编码和执行包括标志寄存器	50%～60%	75%～95%	—
(见注 3)	50%～70%	85%～98%	—
地址计算(见注 3)	50%～60%	60%～90%	85%～98%
程序计数器,栈指针	50%～70%		
	40%～60%		
总线			
存储器管理单元	50%	70%	90%～99%
总监仲裁	50%	70%	90%～99%
中断处理	40%～60%	60%～90%	85%～98%
时钟(石英晶振)(见注 4)	50%	—	95%～99%
程序流监视			
时序(见注 3)	40%～60%	60%～80%	—
逻辑(见注 3)	40%～60%	60%～90%	—
时序和逻辑(见注 5)	—	65%～90%	90%～98%
不可变内存	50%～70%	99%	99.99%
可变内存	50%～70%	85%～90%	99%～99.99%
分立硬件			
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	90%	99.9%	99.99%
机电设备	90%	99%	99.9%
传感器	50%～70%	70%～85%	99%
最终元件	50%～70%	70%～85%	99%

注 1：请参照 GB/T 20438.7—2017 的表 A.1(其给出了需要考虑的失效模式)一起理解本表。

注 2：给定诊断覆盖率范围时,仅当采用了严密地监视方法,或对功能采用了高度动态方式的测试措施时,可取区间上限值。

注 3：对于无高诊断覆盖率数据的技术,目前还没有高效的措施和方法。

注 4：目前石英晶振无中等效果的措施和技术。

请见参考文献的[10]～[12]。

附 录 D
（资料性附录）
E/E/PE 系统中与硬件相关的共因失效影响的量化方法

D.1 概述

D.1.1 介绍

GB/T 20438 中混合使用了许多处理系统性失效的措施。但是无论这些措施有多完善，还是存在发生系统性失效的残余概率。虽然这不会严重影响到单通道系统的可靠性计算，但是多通道系统中可能存在影响多于一个通道（或冗余安全系统的多个部件）的潜在失效，即：共因失效，在对多通道或者冗余系统进行可靠性计算时，会导致实质性错误的结果

本资料性附录描述了两种在多通道或者冗余的 E/E/PE 系统安全评估中考虑共因失效的方法。相对于忽略共因失效的潜在影响而言，使用这些方法给出了对系统完整性更加精确的估算。

第一种方法用来计算共因失效建模中常用的 β 系数。用于在两个或更多系统并行操作的应用中，根据冗余系统中的一个系统的随机硬件失效率估算共因失效的比率（见 D.5）。一般认为，搜集到的随机硬件失效数据中会包含一些系统性失效的影响。

在某些情况下，用替代的方法可能更加适合，例如，从共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，或者受影响的要素超过 4 个。此时就可以使用第二种方法，即二项式失效率（也称冲击模型）方法。

D.1.2 简述

系统的失效被认为是由两种不同原因产生的：

——随机硬件失效；和

——系统性失效。

前者被假设为，对任何部件而言在时间上是随机发生的，并且导致系统某一通道的失效；后者被假设为，当系统达到存在系统性错误的条件时，会立即以确定的方式出现。

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，与单通道失效率相比，同时发生影响并行通道的这种失效的概率是很低的。可以使用成熟的技术计算此概率，但是，如果失效不是彼此完全独立，所得的结果会过于乐观。

相关失效一般被划分为（见参考文献[18]）：

——共因失效（CCF）：由单个的共同的原因引起的多个失效。多个失效可能同时或者在一段时间内发生；

——共模失效（CMF）：一种特殊的共因失效，其中多个设备单位以同一模式失效；

——级联失效：繁衍失效。

CCF 在本附录中经常被用做概括所有的相关失效，他们也被划分为：

——由清晰的确定的原因导致的相关失效。

——由于不够精确，或没有清晰确定的原因，或不可能收集到可靠性数据，而没有在分析中明确考虑的残余的、潜在的多重失效事件。

第一种应该用常规的方式分析、建模和量化，只有第二种应该用附录 D 处理。然而，系统性失

效——完全是相关失效并且在安全分析中没有被识别(否则他们已经被去除)——在 GB/T 20438 中被用特殊的方式加以处理,因此本附录主要是针对硬件随机的相关失效。

因此,由单一原因引起的共因失效,可影响多个通道或者多个部件。它们可能是一个系统性故障引起的(例如:设计或规范的错误)或者由一个外部应力导致的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,共因失效可能会影响多个通道,共因失效的概率就可能成为多通道系统中决定总的失效率的主要因素,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。

D.1.3 共因失效的预防

虽然共因失效是由单一原因导致的,但是它们并不一定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,从而导致共因失效。但所有通道变热的速度不同,临界温度也不同,因此不同通道发生失效的时间各不相同。

可编程系统的架构准许系统在线运行时执行内部诊断测试功能,可使用很多方法,例如:

——一个单通道 PE 系统能够连续检查其内部工作及输入、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%[见参考文献 13]。如果在导致失效之前,99%的内部故障都被揭露出来了,单一通道故障能够最终导致共因失效的概率将大大减少。

——除内部测试之外,多通道 PE 系统中每一个通道均可监视其他通道(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执行交叉监测,发现失效并安全的停车(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,例如旋转机械中经常使用的互锁防护,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,每个通道温度升高速率以及敏感性都有微小差别,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因失效之前启动安全停车。

上述结论如下:

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

——与其他技术相比较,基于 PE 的系统可能适用不同的 β 系数。因此基于历史数据估算的 β 系数很可能是无效的(估算考虑了自动交叉监视影响的共因失效率时,还没有现成的研究模型)。

——因为按时间分布的共因失效,在它们影响到所有通道之前可能就被诊断测试揭露出来了,因此这样的失效不会被识别或者报告为共因失效。

有三种方法可以用来减少潜在的危险共因失效的概率:

a) 减少随机硬件失效和系统性失效的总数(通过缩小图 D.1 中的椭圆面积减少两椭圆相重合的部分)。

b) 使通道最大程度的独立(隔离或者多样化)(在它们的原来面积不变的情况下减少图 D.1 中两椭圆间重合部分的总量)。

c) 在仅有一个通道受到影响,并在下一个通道被影响之前通过诊断测试或者检验测试把共因失效揭露出来。

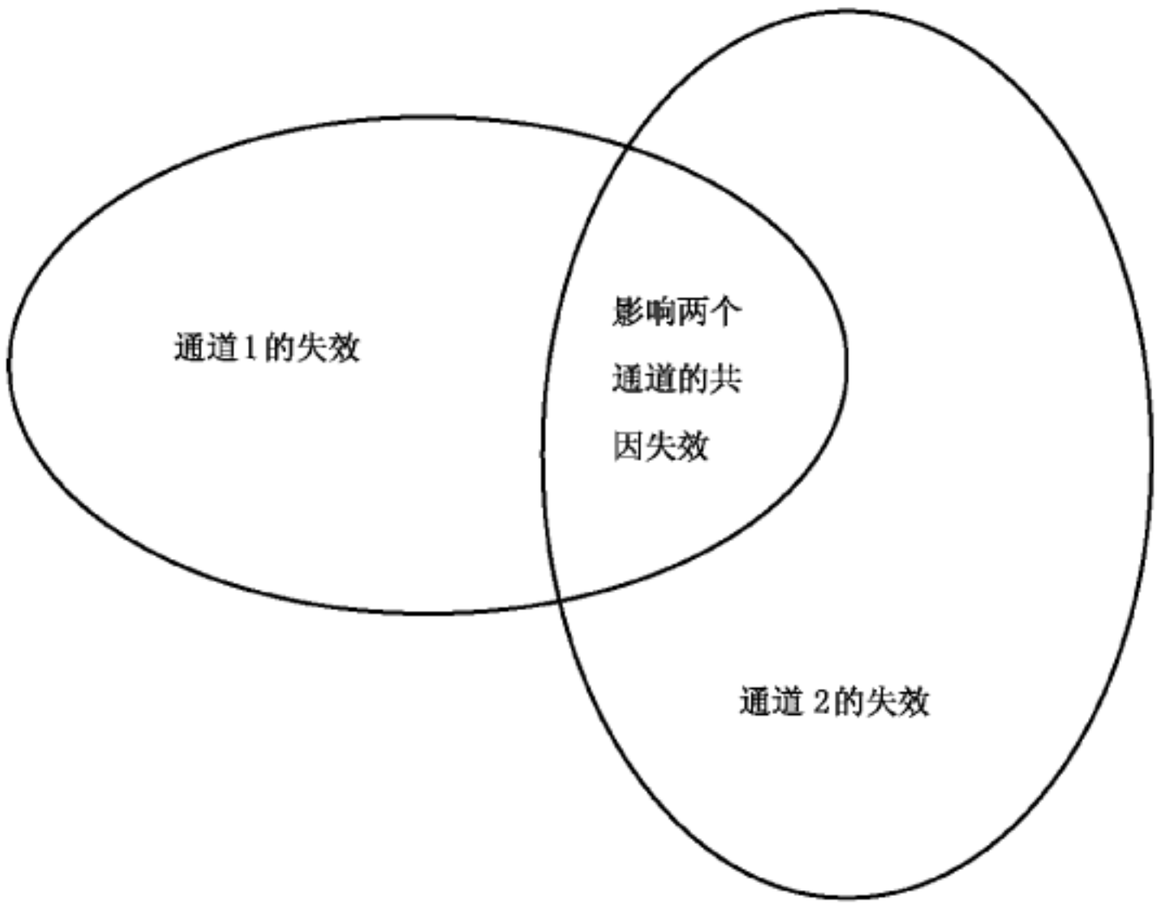


图 D.1　各个通道失效与共因失效的关系

对于多于两个通道的系统，共因失效可能影响全部通道或者仅仅多通道中的几个通道，但这些失效并不都是共同模式引起的。因此根据第一种方法，在本附录是通过计算 1oo2 表决的双重冗余系统的 β 系数，然后根据通道的总数和表决的要求，用倍数因子得到相应的 β 系数。（见表 D.5）

D.1.4　GB/T 20438 中采用的方法

GB/T 20438 以上述三条为基础，采用以下三个步骤：

a）　使用 GB/T 20438.2 和 GB/T 20438.3 中规定的技术，将整个系统性失效的概率减少到与随机硬件失效的概率同级别的水平。

b）　量化那些能够被量化的因素，即，按 GB/T 20438.2 的规定考虑随机硬件失效的概率。

c）　通过目前被认为最实际的途径得出与随机硬件失效率有关的共因失效率的系数。本附录中描述了获得该系数的方法。

大多数估算共因失效率的方法均试图从随机硬件失效率中进行预测。显然，对这些概率之间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率越高，则：

——系统需要的维护量就越高。在维护时引入的系统性故障的概率取决于执行维护的次数，而且这也会对导致共因失效的人为错误率产生影响。这就导致了随机硬件失效率与共因失效率之间的关联。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，这又增加了人为的干扰。

——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，就更易导致系统性故障。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，并会导致部分系统逻辑不能运用（极少的情况除外）。这样也就导致随机硬件失效率与共因失效概率之间的关联。

目前有一些处理 CCF 的方法（β 系数，希腊字母组合，α 系数，二项式失效率…）见参考文献[20]。本附录推荐其中两种方法用于上述的三个步骤的第三步。尽管存在限制，但是相信它们是代表了目前最先进的处理共因失效率的方法：

——广泛使用且完善的 β 系数模型，一般情况下最多能处理四个关联组件的多通道系统。

——二项式故障率见参考文献[21]（即冲击模型）可以用于关联因素高于四个的情况。

下面是在 E/E/PE 系统上使用 β 系数或冲击模型时所遇到的两个难点：

——参数应该选择什么样的值？很多原始资料（例如参考文献[13]）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[14]中最先描述的系统，最近已在参考文献[15]中重新定义。

——β 系数和冲击模型都没有考虑到现代 PE 系统高级的诊断测试能力，这些诊断测试可以用来在非同步共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[14]和[15]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 PE 系统中运行的诊断测试功能不断地将 PE 系统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、部分多样化的、与 PE 系统并行的通道。

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 PE 系统技术，交叉监视能以高重复频率执行。

D.2 方法的使用范围

方法的使用范围局限于硬件的共因失效，其原因如下：

——β 系数和冲击模型将随机硬件失效的概率与共因失效的概率联系起来。整个系统包含的共因失效率并不仅仅取决于硬件，而是取决于系统的复杂性（可能由用户软件决定）。很显然，基于随机硬件失效率的任何计算方式都不考虑软件的复杂性；

——有关共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，一般认为建立系统性失效模型是不可行的（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因失效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率在内的总失效率。

D.3 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高级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因失效，从而在它们影响所有的可用通道之前得以避免。

并不是多通道系统的所有对克服共因失效有影响的特性都能用诊断测试来评价，但诊断测试对于

多样性或独立性相关的这些特性会更有效。非同步共因失效中,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。所以有关克服共因失效的特性可分成两部分:即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因失效的概率可能略小于影响两个通道的失效率,但为了简化 β 系数方法,假设概率是与受到影响的通道数无关的,也就是说,假设当发生一次共因失效时,它将影响所有通道。另一种方法是冲击模型。

没有已知的用于校准这些方法的硬件相关的共因失效数据,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,所以不可能获得与提供主要的控制功能的例行程序一样的质量保证。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.4 使用 β 系数计算 E/E/PE 安全相关系统中共因失效的概率。

考虑在多通道系统中的每一个通道中执行诊断测试时,共因失效对该系统的影响。在应用 β 系数模型时,危险的共因失效的概率为:

$$\lambda_D\beta$$

其中 λ_D 为各个通道随机硬件危险失效率,β 为无诊断测试时的 β 系数,也就是单一通道的失效影响所有通道的比例。

假设共因失效影响所有通道,而且与不同的共因失效相继出现的时间间隔相比,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(从而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(从而总可以通过诊断测试检测到的)。

由危险共因失效引起的总失效率为:

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

其中:

——λ_{DU}:未检测到的单一通道的失效率,即诊断测试覆盖范围之外的失效率,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}:检测到的单一通道的失效率,即在诊断测试范围内单一通道的失效率;如果诊断测试的重复率高,则失效部份会被揭露出来,从而导致 β 值减少,即 β_D 值;

——β_D:可检测到的危险故障的共因失效系数。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:可从引用表 D.4 结果的表 D.5 中获得,计算公式为 $S=X+Y$(见 D.5);

——β_D:可从引用表 D.4 结果的表 D.5 中获得,计算公式为 $S_D=X(Z+1)+Y$。

D.5 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。

为了最大限度的减小发生共因失效的概率，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将大量的诊断测试结合进来，从而允许检测非同步发生的共因失效。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因失效的作用的程度。

表 D.1 的使用者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。

表 D.2 和 D.3 可以用于根据诊断测试的频率和覆盖率决定系数 Z，并考虑到重要的注 4(它限制了何时才可使用非零 Z 值)的情况。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_{int} 的值(未检测到的故障的 β 系数)；

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

这里，用 S 或 S_D 在表 D.4 中确定相应的 β_{int} 系数值。

β_{int} 和 β_{Dint} 是考虑了不同冗余度影响之前的共因失效值。

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有有效的物理隔离方式？例如，置于各自的机柜中。	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
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位于室内并且在各自的机柜里？			2.5	0.5
多样性与冗余				
各通道是否使用不同的电气技术？例如一个使用电子、可编程电子技术，另外的使用继电器技术。	8.0			
各通道是否使用不同的电子技术？例如一个使用电子技术，另外一个使用可编程电子技术。	6.0			
设备的传感器件是否使用不同的物理原理，例如压力和温度，叶片式风速计和多普勒变送器等。			9.0	
设备是否使用不同的电气原理/设计方案？例如数字的或模拟的、不同的制造商(不重复贴牌的)或不同的技术。			6.5	
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		

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}
多样性与冗余				
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	2.0		
各通道是否是由在设计期间没有任何交流的不同的设计人员设计的？	1.5	1.5		
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	2.0
每个通道的维护是否是由不同的人员在不同的时间进行的？	3.0		3.0	
复杂性/设计/应用/成熟度/经验				
通道之间的交叉连接是否能排除任何信息交换，除非是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，是否是基于在该领域已成功使用 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？例如每个通道不超过 10 个输入或输出。		1.0		
输入和输出是否具有对潜在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降额(例如，不小于 2)？	2.0		2.0	
评估/分析及数据反馈				
是否对为确立共因失效源而进行的失效模式及影响分析或故障树分析的结果进行检查，并且是否已通过设计消除了事先确定的共因失效源？		3.0		3.0
设计复审过程中，是否考虑了将共因失效的结果反馈到设计当中？(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				
是否有记录系统可以用来确保记录检测到的所有部件的失效(或退化)、已了解的根源或类似潜在失效原因的项目？		1.5	0.5	1.5
是否存在以下规程：独立通道中任一部分的维护(包括调节或校准)都是交叉进行的，并且除了执行维护之后的手动检查，允许在完成一个通道的维护与另一个通道开始进行维护之间可靠地运行诊断测试？	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，并不会被重新布置？	0.5	0.5	0.5	0.5
是否所有印制电路板等的维护均在现场外有资质的维修中心执行，而且，是否所有修复项目均通过了安装前的测试？	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}
规程/人工接口				
系统是否为低诊断覆盖率(60%～90%)？并且失效报告是否详细到现场可更换模块级？	0.5			
系统是否为中等诊断覆盖率(90%～99%)？并且失效报告是否详细到现场可更换模块级？	1.5	1.0		
系统是否为高诊断覆盖率（>99%)？并且失效报告是否详细到现场可更换模块级？	2.5	1.5		
系统诊断测试报告的失效是否详细到现场可更换模块级？			1.0	1.0
能力/培训/安全文化				
设计人员是否经过培训(具有培训文档)，从而理解了共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(具有培训文档)，从而理解了共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(如上锁的机柜与不允许接近的位置)？	0.5	2.5	0.5	2.5
在无额外环境控制的情况下，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、湿度等)的抗干扰性是否按照认可标准中规定的水平进行了测试？	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，规程就位。在随附的文档中，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：

注 3：——制造商在受控条件下进行修理，而不是在现场不太合适的条件下进行(可能是错误的)修理。这样，因为减小了系统失效(因此也减小了共因失效)的概率，从而对 Y 列作出了一定贡献；

注 4：——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输入。

表 D.2　Z 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 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 天	2 天～1 周	大于 1 周
≥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：如果对表 D.1 中的分类目录进行均衡考虑,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,需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:具有分离机架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机架中?”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,就被视为传感器或最终元件。

注 4：对于使用非零 Z 值,确保在非同步共因失效影响所有通道之前使受控设备进入安全状态。同时达到安全状态所需的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,系统启动自动停车;或

——在第一次故障后,并不启动安全停车[9],而诊断测试能:

- 确定故障位置,能给故障定位;且
- 具有发现任何后续故障时,继续将 EUC 置于安全状态的能力;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,一个正式的工作规程已就位,并且:

- 如果故障可能导致共因失效,需立即关闭设备;或
- 在声明的诊断测试间隔中,修复了有故障的通道。

注 5：过程工业中,当在诊断测试间隔(如表 D.2 中所描述)中发现故障时,关闭 EUC 似乎是不合适的。这种方法不被曲解为: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_{int} 和 β_{Dint} 的计算

得分(S 或 S_D)	β_{int} 或 β_{Dint} 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_{Dint} 最大水平比平常使用中低,是因为使用了在 GB/T 20438 中其他地方所规定的技术,从而降低整体的系统失效的概率以及由系统失效导致的共因失效的概率。 **注 2**：逻辑子系统中小于 0.5% 的 β_{Dint},传感器中小于 1% 的 β_{Dint} 的合理性是很难证明的。		

9)　宜考虑识别不同故障时系统的操作。例如,当识别出单一故障后,对于一个简单的 2oo3 系统宜在表 D.2 和 D.3 中标出的时间内关闭。如果系统没有关闭,第二通道的失效将导致两个有故障的通过否决掉其余的(正常的)通道。在一个通道出现故障时,可自动重新配置成 1oo2 有决的,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。

表 D.4 中得到的 β_{int} 值是与 1oo2 系统的共因失效相关的。对于其他的冗余($MooN$),根据表 D.5 对 β_{int} 进行调整以获得最后的 β 值。

表 D.5 也可以用来确定最后的 β_D 的值,但要将 β_{int} 替换成 β_{Dint}。

注 7:相关信息(PDS 方法)见参考文献[25]。

表 D.5 冗余级别高于 1oo2 的系统的 β 的计算

$MooN$		N			
		2	3	4	5
M	1	β_{int}	$0.5\beta_{int}$	$0.3\beta_{int}$	$0.2\beta_{int}$
	2		$1.5\beta_{int}$	$0.6\beta_{int}$	$0.4\beta_{int}$
	3			$1.75\beta_{int}$	$0.8\beta_{int}$
	4				$2\beta_{int}$

D.6 β 系数方法使用的示例

为了演示使用此方法的效果,表 D.6 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。这些值是分类的最大分值的一半。

在多样化系统示例中。多样性/冗余类别的值可以通过考虑表 D.1 中该类所列的各项属性得出:

——其中一个系统为电子系统,另一个使用继电器技术;

——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,总共会产生四种示例系统。

表 D.6 可编程电子的示例值

类别		有良好诊断测试的多样化系统	缺乏诊断测试的多样化系统	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

表 D.6（续）

类别		有良好诊断测试的多样化系统	缺乏诊断测试的多样化系统	拥有良好诊断测试的冗余系统	缺乏诊断测试的冗余系统
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%
多样化系统 1oo2(表 D.5)冗余系统是三重的 2oo3 表决系统(表 D.5)		0.5%	2%	1.5%	7.5%

D.7 二项式失效率(冲击模型)-CCF 方法

共因失效(CCF)现场反馈表明，出现过许多双重失效，一些三重失效，也许有一个四重失效，但是由于明确的单个原因(在安全分析中未识别出的)引起四重以上失效从未发现过。结论是，当 CCF 的重数增加的时候，多个相关失效的概率降低。因此，如果 β 系数模型对于双重失效是切实可行的，对于三重失效有点保守的话，那么对于四重失效甚至更高重的失效来说就过于保守了。我们来看一个典型的安全仪表系统，此系统用于油田中，当出口发生堵塞的时候将 n(例如 $n=150$)个生产井关断。当然可能有 2 个、3 个甚至 4 个井源于不明确的 CCF 而无法关断，而并不是 β 系数建模中的 n 个井(否则 CCF 会是明显的并且应该作为单个故障进行分析)。另一个典型的例子发生在同一时间处理多个安全层。例如，如果考虑两个安全层传感器之间潜在的 CCF，可能意味着要考虑 6 个传感器之间的 CCF。(即：每个层 3 个传感器)。

已经推荐了一些模型见参考文献[18]用于处理此类难点，但是大多数都需要许多可靠性的数据(例如：希腊字母组合和 α 模型)，因此就不是很实用。其中，由维赛利(Vesely)在 1977 年提出并由阿特伍德(Atwood)在 1986 年改进的二项式失效率(冲击模型)提供了一个实用的解决方案见参考文献[18，19]。原理就是当一个 CCF 发生的时候，就像对相关的部件产生了冲击。冲击可能是致命的(与 β 系数模型中一样的冲击)也可能是非致命的，在这样情况下由于冲击导致给定的部件失效只有一个确定的概率，这样非致命性的冲击产生的 k 个失效的概率是以二项式的形式分布的。

这个模型仅需要 3 个参数就可以完成：

——ω 致命的冲击率；

——ρ 非致命的冲击率；

——γ 在给定的非致命的冲击下部件失效的条件概率。

图 D.2 中给出了使用故障树执行这种方法的一个示例。

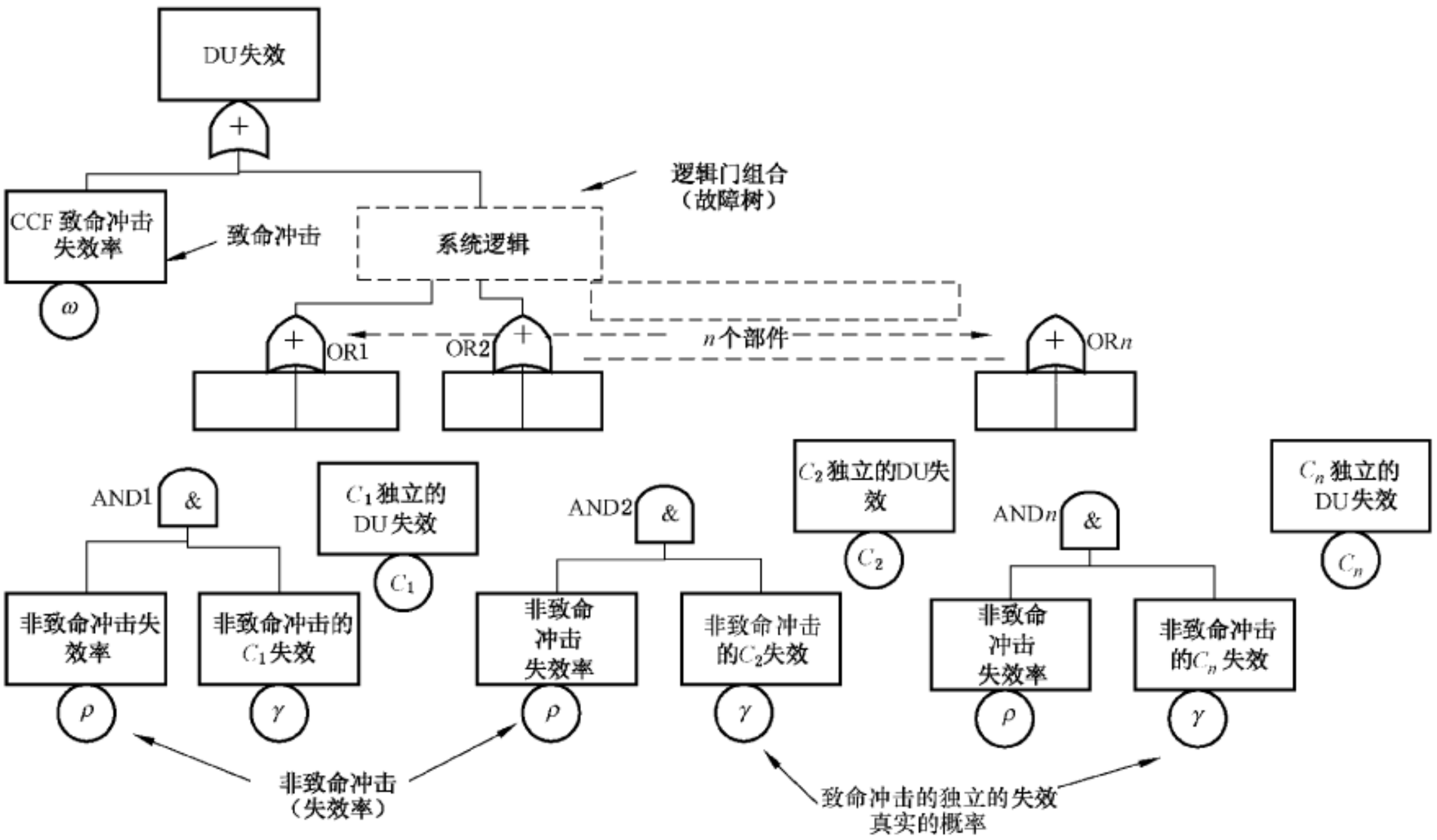


图 D.2　冲击模型的故障树实现

通过把 β 分成 β_L 和 β_{NL} 两部分，相同的部件能够连接到 β 系数模型：

——$\beta=\beta_L+\beta_{NL}$

——致命冲击的失效率：$\lambda_{DU}\times\beta_L$

——非致命冲击的失效率：$\lambda_{DU}\times B_{NL}$

——独立的失效率：$\lambda_{DU}[1-(\beta_L+\beta_{NL})]$

在图 D.2 故障树中，它变为：

——致命冲击率：$\omega=\lambda_{DU}\times\beta_L$

——非致命冲击率：$\rho=\lambda_{DU}\times B_{NL}/\gamma$

通常，主要的问题是评估三个参数的值(ω,ρ,γ)或者$(\beta_L,\beta_{NL},\gamma)$。参考文献[19]给出了说明并且提供了其他一些参考文献，是有关可以通过现场反馈来评估(ω,ρ,γ)的统计学处理方法。

如果没有有用的数据，可以使用实际的工程判断。例如当出现 3 个以上同类项，可按以下步骤进行故障树建模：

1)　与 β 系数方法一样估计 β 值；

2)　考虑 β_L 是可以忽略的$(\beta_{NL}=\beta)$

3)　为了取得保守的结果而评估 γ。考虑双重失效至少会产生比四重失效高 10 倍的冲击(保守的假设)，可以使用如下的公式：

$$\gamma=\sqrt{\frac{C_N^2}{10C_N^4}} \qquad \cdots\cdots(1)$$

式中：

N ——同类项的数量；

C_N^2——潜在的双重失效的数量；

C_N^4——潜在的四重失效的数量。

4) 使用含有同类项数量 N 的函数计算 ρ：

$$\rho = \frac{\beta\lambda_{DU}}{C_N^2\gamma^2 + C_N^3\gamma^3}$$

在这种方法的使用中，双重和三重失效是突出的贡献者，并且，与仅使用 3 个部件的 β 系数方法比较，结果是保守的。考虑 CCF 的双重和三重失效时，也没有完全忽略不现实的多重失效。

这种模型易用于诸如附录 B 中所示的故障树计算模型，例如：B.4.3 的故障树。这种方法可以用非常简单和容易的方法处理包含多个相同部件的安全系统。

D.8 参考文献

参考文献中[13]～[15]，[20]和[21]提供了共因失效的相关信息。

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

此附录给出了应用软件安全完整性表的两个工作示例，这些表格由 GB/T 20438.7—2017 的附录 A 规定：

a） 安全完整性等级 2：化工厂生产过程所需的可编程电子安全相关系统。

b） 安全完整性等级 3：基于高级语言的停车应用程序。

这些例子阐述了在 GB/T 20438.7—2017 附录 A 和附录 B 的表格所列特定情况中能够选择何种软件开发技术。

应该强调的是这些阐述并不是标准对这些示例的确定的应用。GB/T 20438.3 在许多地方都清楚的表明，由于存在大量影响软件系统性能力的因素，所以无法给出对于任何特定应用都正确的，组合了技术和措施的算法。

对于真实的系统，表格中的所有项都应该有文档化的论证作为支持，以做出正确的注释并对于特定的系统和应用表明其相应的响应。此论证类似于通过引用 GB/T 20438.7—2017 附录 C 的指南获得的辅助，指南中讨论了某些可取的属性，它们如果在适当的生命周期阶段实现，则可充分证明最终的软件具有足够的系统安全完整性。

E.2 安全完整性等级 2 的示例

此例是一个安全完整性等级 2 的可编程电子安全相关系统在化工厂的生产过程的中应用。可编程电子安全相关系统利用梯形图编写应用程序，是一个有限可变语言应用编程的示例。

此应用由几个反应容器组成，它们由一些中间储存容器相连，在反应周期中的某些点对其充入惰性气体以避免着火和爆炸。可编程电子安全相关系统的功能包括：按安全要求规范的要求，接收来自传感器的输入，为阀门、泵和执行器供电并互锁，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；

——危险和风险分析已确定在本应用中需要安全完整性等级为 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式控制系统的接口；

——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审查，但已证实其能达到 GB/T 20438.3 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；

——软件开发的全过程已由独立于软件开发小组的人员进行复审；

——确认测试已由独立于软件开发小组的人员见证和批准；

——修改（如果需要）要由独立于软件开发小组的人员来授权；

注 1：有关独立人员的定义，见 GB/T 20438.4。

注 2：当使用有限可变编程时，PLC 供应商和用户之间的职责划分的信息，参考中 GB/T 20438.7—20177.4.2，7.4.3，7.4.4 和 7.4.5 的注释。

如下表格给出了 GB/T 20438.7—2017 附录 A 在本应用如何具体使用。

表 E.1　软件安全要求规范

（见 GB/T 20438.3—2017 的 7.2）

	技术/措施	Ref.	SIL2	在本应用中的解释
1a	半形式化方法	表 B.7	R	因果图，顺序图，功能块。典型地用于 PLC 应用软件要求规范
1b	形式化方法	B.2.2 C.2.4	R	不用于有限可变编程
2	在系统安全要求和软件安全要求间向前可追溯	C.2.11	R	检查完整性：复核以确保软件安全要求表达了所有的系统安全要求
3	在安全要求和认识到的安全需求间向后可追溯	C.2.11	R	最小化复杂性和功能性：复核以确保所有的软件安全要求确实是表达系统安全要求所必须的
4	支持上述适当的技术或措施的计算机辅助规范工具	B.2.4	R	由 PLC 厂家提供的开发工具
注 1：在参考列（题头为 ref.），资料性的参考“B.x.x.x”，“C.x.x.x” 是指在 GB/T 20438.7—2017 的附录 B 和附录 C 中技术的描述，同时“Table A.x”，“Table B.x”是指 GB/T 20438.7—2017 的附录 A 和附录 B 的技术表格。 注 2：用自然语言说明软件安全要求。				

表 E.2　软件设计与开发：软件架构设计

（见 GB/T 20438.3—2017 的 7.4.3）

	技术/措施	Ref.	SIL2	在本应用中的解释
1	故障检测	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	错误检测代码	C.3.2	R	以用户选项嵌入——谨慎选择
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某些基本安全条件（见 1）
3b	多样化监视技术（同一台计算机上的监视功能和被监视功能之间独立）	C.3.4	R	不优选：为了保证独立性增加了软件的复杂程度
3c	多样化监视技术（监视计算机与被监视计算机之间分离）	C.3.4	R	在独立的硬件安全监控器中检查合法的输入/输出的组合
3d	多样化冗余，实现相同软件安全要求规范	C.3.5	R	不优选：安全效益的增加不超过 3c
3e	功能上多样化冗余，实现不同软件安全要求规范	C.3.5	R	不优选：实质上是由 3c 实现的

表 E.2（续）

	技术/措施	Ref.	SIL2	在本应用中的解释
3f	后向恢复	C.3.6	R	以用户选项嵌入——谨慎选择
3g	无状态软件设计(或者有限状态设计)	C.2.12	—	不使用。过程控制需要状态以记住工厂的条件
4a	故障恢复重试机制	C.3.7	R	根据应用的需求使用(见 2 和 3c)
4b	适度降级	C.3.8	R	不用于有限可变编程
5	人工智能——故障纠正	C.3.12	NR	不用于有限可变编程
6	动态再配置	C.3.13	NR	不用于有限可变编程
7	模块化方法	表 B.9	HR	
8	使用可信赖/已证实的软件组件(如可获得)	C.2.10	HR	来自较早项目的已有代码
9	在软件安全要求规范和软件架构间向前的追溯性	C.2.11	R	检查完整性:复核以确保所有的软件安全要求都由软件架构表达了
10	在软件安全要求规范和软件架构间向后的追溯性	C.2.11	R	最小化复杂性和功能性:复核以确保所有的架构安全需求确实是表达软件安全要求所必须的
11a	结构化的图解方法	C.2.1	HR	至少用数据流方法和数据的逻辑表格来表示设计架构
11b	半形式化方法	表 B.7	R	可用于 DCS 的接口
11c	形式化设计和优化方法	B.2.2 C.2.4	R	很少用于有限可变编程
11d	自动软件生成	C.4.6	R	不用于有限可变编程
12	计算机辅助规范和设计工具	B.2.4	R	由 PLC 厂商提供的开发工具
13a	周期性运转,并且确定最大周期时间	C.3.11	HR	不使用。PLC 循环时间有硬件监控
13b	时间触发式架构	C.3.11	HR	不使用。PLC 循环时间有硬件监控
13c	事件驱动,并且确定最大响应时间	C.3.11.	HR	不使用。PLC 循环时间有硬件监控
14	静态资源分配	C.2.6.3	R	不使用。动态的资源问题不会出现在有限可变编程中
15	访问共享资源的静态同步	C.2.6.3	—	不使用。动态的资源问题不会出现在有限可变编程中

注 1：在参考列(题头为 ref.),资料性的参考“B.x.x.x”,“C.x.x.x” 是指在 GB/T 20438.7—2017 的附录 B 和附录 C 中技术的描述,同时“Table A.x“,””Table B.X”是指的 GB/T 20438.7—2017 附录 A 和附录 B 的技术表格。

注 2：在有限可变的编程中使用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 20438.2—2017 的 7.4.4)

技术/措施		Ref.	SIL2	在本应用中的解释
1	适当的编程语言	C.4.5	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	不用。使用面向 PLC 的结构化文本(见参考文献[16])
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	已认证的工具和已认证的翻译器	C.4.3	HR	可从某些 PLC 供应商处买到
4b	工具和翻译器:通过使用提高置信度	C.4.4	HR	PLC 供应商的开发工具包;经过若干项目开发的内部工具
注:在参考栏(题头为 Ref.),资料性的参考"B.x.x.x","C.x.x.x"是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述,而"Table A.x","Table B.x"指的是在 GB/T 20438.7—2017 附录 A 和附录 B 中的技术表格。				

表 E.4　软件设计与开发:详细设计

(见 GB/T 20438.2—2017 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	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	形式化设计和优化方法	B.2.2 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	模块化方法	表 B.9	HR	将 PLC 程序梯形逻辑排序和分组,按照功能要求的考虑达到最大程度的模块化
5	设计和编码标准	C.2.6 表 B.1	HR	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/经验证的软件组件(如可获得)	C.2.10	HR	功能块,部分程序
8	在软件安全要求规范和软件设计间向前可追溯	C.2.11	R	检查完整性:复审,以确保软件设计表达了所有的软件安全要求
注:在参考栏(题头为 Ref.),资料性的参考"B.x.x.x","C.x.x.x"是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述,而"Table A.x","Table B.x"指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。				

表 E.5　软件设计和开发:软件模块测试和集成

(见 GB/T 20438.3—2017 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
4	功能和黑盒测试	B.5.1 B.5.2 表 B.3	HR	选择输入数据以便执行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	性能测试	表 B.6	R	不用于有限可变编程
6	基于模型的测试	C.5.27	R	不用于有限可变编程
7	接口测试	C.5.3	R	包括在功能和黑盒测试中
8	测试管理和自动化工具	C.4.7	HR	PLC 制造商提供开发工具
9	在软件设计规范与模块及集成测试规范间向前可追溯	C.2.11	R	检查完整性:复审,以确保规划了足够的测试来检查所有的模块及其相关模块集成的功能性
10	形式化验证	C.5.12	—	不用于有限可变编程

注:在参考栏(题头为 Ref.),资料性的参考“B.x.x.x”,“C.x.x.x”是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述,而“Table A.x”,“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。

表 E.6　可编程电子集成(硬件和软件)

(见 GB/T 20438.3—2017 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	选择输入数据以便执行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	表 B.6	R	装配 PLC 系统时用于工厂验收测试
3	在系统及针对硬件/软件集成的软件设计要求和硬件/软件集成测试规范之间向前可追溯	C.2.11	R	复审以确保硬件/软件集成测试是足够的

注:在参考栏(题头为 Ref.),资料性的参考“B.x.x.x”,“C.x.x.x”是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述,而“Table A.x”,“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。

表 E.7　系统安全确认的软件方面）

（见 GB/T 20438.3—2017 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
2	过程仿真	C.5.18	R	不用于有限可变编程，但是更普遍用于 PLC 系统开发
3	建模	表 B.5	R	不用于有限可变编程，但是更普遍用于 PLC 系统开发
4	功能和黑盒测试	B.5.1 B.5.2 表 B.3	HR	选择输入数据以便执行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	在软件安全要求规范和软件安全确认计划间向前可追溯	C.2.11	R	检查完整性：复审以确保规划了足够的软件确认测试已表达软件安全要求
6	在软件安全确认计划和软件安全要求规范间向后可追溯	C.2.11	R	最小化复杂性：复审以确保所有的确认测试是有实质作用的
注：在参考栏（题头为 Ref.），资料性的参考“B.x.x.x”，“C.x.x.x” 是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述，而“Table A.x”，“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。				

表 E.8　软件修改

（见 GB/T 20438.3—2017 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的模块化如何限制打算进行的修改所产生的影响
2	再验证被变更的软件模块	C.5.23	HR	重复以前的测试
3	再验证受影响的软件模块	C.5.23	HR	重复以前的测试
4a	再确认整个系统	表 A.7	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
4b	回归确认	C.5.25	HR	
5	软件配置管理	C.5.24	HR	基线，改变记录，对其他系统要求的影响
6	数据记录和分析	C.5.2	HR	测试用例和结果的记录
7	在软件安全要求规范和软件修改计划（包括再验证和再确认）之间向前可追溯	C.2.11	R	足够的修改规程以实现软件安全要求
8	软件修改计划（包括再验证和再确认）和软件安全要求规范之间向后可追溯	C.2.11	R	足够的修改规程以实现软件安全要求
注：在参考栏（题头为 Ref.），资料性的参考“B.x.x.x”，“C.x.x.x” 是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述，而“Table A.x”，“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。				

表 E.9 软件验证

（见 GB/T 20438.3—2017 的 7.9）

技术/措施		Ref.	SIL2	在本应用中的解释
1	形式化证明	C.5.12	R	不用于有限可变编程中
2	规范和设计的动画演示	C.5.26	R	
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	自动测试装置以促进回归测试
5	软件设计规范和软件验证(包括数据验证)计划之间向前可追溯	C.2.11	R	检查完整性:复审以确保足够的功能测试
6	软件验证(包括数据验证)计划和软件设计规范之间向后可追溯	C.2.11	R	最小化复杂性:复审以确保所有的验证测试是有实质作用的
7	离线数值分析	C.2.13	R	不被使用。计算的数值稳定性在这里不是一个关注的焦点
软件模块测试和集成		见本部分的表 E.5		
可编程电子集成测试		见本部分的表 E.6		
软件系统测试(确认)		见本部分的表 E.7		

注：在参考栏(题头为 Ref.),资料性的参考“B.x.x.x”，“C.x.x.x” 是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述,而“Table A.x”，“Table B.x”指的是在 GB/T 20438.7—2017 附录 A 和附录 B 中的技术表格。

表 E.10 功能安全评估

（见 GB/T 20438.3—2017 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	使用
2	判定/真值表	C.6.1	R	有限度使用
3	失效分析	表 B.4	R	在系统层使用因果图,但在其他方面,对于有限可变编程不使用失效分析
4	多样化软件的共因失效分析(如实际使用了多样化软件)	C.6.3	R	不用于有限可变编程中
5	可靠性框图	C.6.5	R	不用于有限可变编程中
6	第 8 章要求和软件功能安全评估计划之间的向前可追溯	C.2.11	R	检查功能安全评估的覆盖率完整性

注：在参考栏(题头为 Ref.),资料性的参考“B.x.x.x”，“C.x.x.x” 是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述,而“Table A.x”，“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。

E.3 安全完整性等级 3 的示例

第二个例子是一个基于高级语言的停车应用程序，它的安全完整等级是 3。

就安全相关系统而言，这个软件系统是相对较大的；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来自以往项目的已有代码(经使用证实的)。总之，如果这些都可用，则系统包含了 100 000 多行源代码。

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以逻辑与(AND) 进行连接。

假设：

——虽然不需要快速响应，但是要保证最大的响应时间；

——具有到传感器、执行器和对操作人员的报警器接口；

——得不到操作系统、图形例程、商业数学例程的源代码；

——系统很可能有进一步的改变；

——使用一种通用程序语言来开发一些特殊软件；

——系统是部分面向对象的；

——所有得不到源代码的部分要以多样性实现，使用从不同供货商处得来的软件部件，并由多种翻译器生成目标代码；

——软件在几个能满足 GB/T 20438.2 要求的，市场上可得到的处理器上运行；

——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：关于独立组织的定义见 GB/T 20438.4。

以下表格说明了针对本应用如何解释 GB/T 20438.7—2017 的附表。

表 E.11 软件安全要求规范

(见 GB/T 20438.3—2017 的 7.2)

技术/措施		Ref.	SIL3	在本应用中的解释
1a	半形式化方法	表 B.7	HR	框图、时序图、状态转换图
1b	形式化方法	B.2.2 C.2.4	R	仅在特殊情况下使用
2	在系统安全要求规范和软件安全要求间向前可追溯	C.2.11	HR	检查完整性：复审以确保所有的系统安全要求已由软件安全要求表达
3	在软件安全要求规范和获知到的安全要求间向后可追溯	C.2.11	HR	最小化复杂性和功能：复审以确保所有的软件安全要求对于表达系统安全要求是确实需要的
4	支持上述适当的技术或措施的计算机辅助规范工具	B.2.4	HR	支持选定方法的工具
注：在参考栏(题头为 Ref.)，资料性的参考“B.x.x.x”，“C.x.x.x” 是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述，而“Table A.x”，“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。				

表 E.12　软件设计与开发:软件架构设计

(见 GB/T 20438.3—2017 的 7.4.3)

技术/措施		Ref.	SIL3	在本应用中的解释
1	故障检测	C.3.1	HR	用于处理传感器、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	错误检测代码	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	多样化监视技术(同一台计算机上的监视功能和被监视功能之间独立)	C.3.4	R	不是首选:为保证独立性而增加软件复杂性
3c	多样化监视技术(监视计算机与被监视计算机之间分离)	C.3.4	R	用于一些在 3a 中没被使用的安全相关功能
3d	多样化冗余,实现相同软件安全要求规范	C.3.5	—	用于某些源代码不可得到的功能
3e	功能上多样化冗余,实现不同软件安全要求规范。这通常要求传感器在不同的物理原理下运行	C.3.5	R	不是首选:大体上由 3c 实现
3f	后向恢复	C.3.6	—	不使用
3g	无状态设计(或者有限状态设计)	C.2.12	R	不使用。一个受控停车需要用状态来记忆装置条件
4a	故障恢复重试机制	C.3.7	—	不使用
4b	适度降级	C.3.8	HR	是,因为工艺过程的固有特性
5	人工智能——故障纠正	C.3.9	NR	不使用
6	动态再配置	C.3.10	NR	不使用
7	模块化方法	表 B.9	HR	需要,由于系统的规模
8	使用可信赖/已证实的软件模块和组件(如可获得)	C.2.10	HR	以往项目中的已有代码
9	在软件安全要求规范和软件架构间向前可追溯	C.2.11	HR	复审以确保软件架构表达了所有的软件安全要求
10	在软件安全要求规范和软件架构间向后可追溯	C.2.11	HR	最小化复杂性和功能:复审以确保所有的架构安全要求对于表达软件安全要求是确实需要的
11a	结构图表的方法	C.2.1	HR	需要,由于系统的规模
11b	半形式化方法	表 B.7	HR	框图、时序图、状态转换图
11c	形式化设计和优化方法	B.2.2 C.2.4	R	不使用

表 E.12（续）

技术/措施		Ref.	SIL3	在本应用中的解释
11d	自动软件生成	C.4.6	R	不使用。消除编译器/生成器的不确定性
12	计算机辅助规范和设计工具	B.2.4	HR	支持选定方法的工具
13a	周期性运转，并且确定最大周期时间	C.3.11	HR	不使用
13b	时间触发式架构	C.3.11	HR	不使用
13c	事件驱动，并且确保最大响应时间	C.3.11	HR	不使用
14	静态资源分配	C.2.6.3	HR	不使用。选择编程语言以消除动态资源问题
15	访问共享资源的静态同步	C.2.6.3	R	不使用。选择编程语言以消除动态资源问题

注：在参考栏(题头为 Ref.)，资料性的参考“B.x.x.x”，“C.x.x.x”是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述，而“Table A.x”，“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。

表 E.13 软件设计与开发：支持工具及编程语言

（见 GB/T 20438.3—2017 的 7.4.4）

技术/措施		Ref.	SIL3	在本应用中的解释
1	适当的编程语言	C.4.6	HR	选择全可变高级语言
2	强类型编程语言	C.4.1	HR	已使用
3	语言子集	C.4.2	HR	对选择的语言定义子集
4a	已认证的工具	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

注：在参考栏(题头为 Ref.)，资料性的参考“B.x.x.x”，“C.x.x.x”是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述，而“Table A.x”，“Table B.x”指的是在 GB/T 20438.7—2017 附录 A 和附录 B 中的技术表格。

表 E.14 软件设计与开发：详细设计

（见 GB/T 20438.3—2017 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	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/状态迁移图、框图、顺序图
1c	形式化设计和优化方法	B.2.2 C.2.4	R	仅针对一些很基本的元件，仅在特殊情况下使用
2	计算机辅助设计工具	B.3.5	HR	用于所选择的方法

表 E.14（续）

技术/措施		Ref.	SIL3	在本应用中的解释
3	防御性编程	C.2.5	HR	除了编译器自动插入，所有措施均在它们起作用的应用软件中显式使用
4	模块化方法	表 B.9	HR	限制软件模块大小，信息隐藏/封装，在子程序和函数中设置单入口/单出口，完全定义的接口……
5	设计和编码标准	C.2.6 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	使用可信的/经验证的软件组件（如可获得）	C.2.10	HR	可得到并已使用
8	在软件安全要求规范和软件设计间向前可追溯	C.2.11	HR	复审以确保软件设计表达了所有的软件安全要求
注：在参考栏（题头为 Ref.），资料性的参考“B.x.x.x”，“C.x.x.x”是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述，而“Table A.x”，“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。				

表 E.15　软件设计与开发：软件模块测试和集成

（见 GB/T 20438.3—2017 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使用于软件模块
2	动态分析和测试	B.6.5 表 B.2	HR	在可得到源代码时用于软件模块。测试用例来自边界值分析，性能建模，等价类和输入划分，基于结构的测试
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，以便执行所有功能用例（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	性能测试	表 B.6	HR	在对目标硬件进行集成测试期间使用
6	基于模型的测试（MBT）	C.5.27	HR	不使用
7	接口测试	C.5.3	HR	包含在功能和黑盒测试中
8	测试管理和自动化工具	C.4.7	HR	可获得的地方使用
9	在软件设计规范与模块及集成测试规范间向前可追溯	C.2.11	HR	复审以确保集成测试是足够的
10	形式化验证	C.5.12	R	不使用
注：在参考栏（题头为 Ref.），资料性的参考“B.x.x.x”，“C.x.x.x”是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述，而“Table A.x”，“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。				

表 E.16　可编程电子集成(硬件和软件)

(见 GB/T 20438.3—2017 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	作为软件集成测试的附加测试(见表 E.15)使用。 选择输入数据,以便执行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	性能测试	表 B.6	HR	广泛地使用
3	在系统及针对硬件/软件集成的软件设计要求和硬件/软件集成测试规范之间向前可追溯	C.2.11	HR	复审以确保集成测试是足够的
注:在参考栏(题头为 Ref.),资料性的参考“B.x.x.x”,“C.x.x.x”是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述,而“Table A.x”,“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。				

表 E.17　软件方面的系统安全确认(软件安全确认)

(见 GB/T 20438.3—2017 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	不用于确认
2	过程仿真	C.5.18	HR	有限状态机,性能建模,原型设计和动画
3	建模	表 B.5	HR	不用于确认
4	功能和黑盒测试	B.5.1 B.5.2 表 B.3	HR	选择输入数据,以便执行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
5	在软件安全要求规范和软件安全确认计划间的向前可追溯	C.2.11	HR	检查完整性:复审以确保确认计划已表达所有的软件安全要求
6	在软件安全确认计划和软件安全要求规范间的向后可追溯	C.2.11	HR	最小化复杂性:复审以确保所有的确认测试是有实质作用的
注:在参考栏(题头为 Ref.),资料性的参考“B.x.x.x”,“C.x.x.x”是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述,而“Table A.x”,“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。				

表 E.18　修改

（见 GB/T 20438.3—2017 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	已使用
2	再验证被变更的软件模块	C.5.23	HR	已使用
3	再验证受影响的软件模块	C.5.23	HR	已使用
4a	再确认整个系统	表 A.7	HR	根据影响分析的结果
4b	回归确认	C.5.25	HR	已使用
5	软件配置管理	C.5.24	HR	已使用
6	数据记录和分析	C.5.2	HR	已使用
7	在软件安全要求规范和软件修改计划（包括再验证和再确认）之间的向前可追溯	C.2.11	HR	检查完整性：复审以确保修改规程足以达到软件安全要求
8	软件修改计划（包括再验证和再确认）和软件安全要求规范之间的向后可追溯	C.2.11	HR	最小化复杂性：复审以确保所有的修改规程是必要的

注：在参考栏（题头为 Ref.），资料性的参考“B.x.x.x”，“C.x.x.x”是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述，而“Table A.x”，“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。

表 E.19　软件验证

（见 GB/T 20438.3—2017 的 7.9）

技术/措施		Ref.	SIL3	在本应用中的解释
1	形式化证明	C.5.12	R	仅在特殊情况下，仅用于一些基本的类
2	规范和设计的动画演示	C.5.26	R	不使用
3	静态分析	B.6.4 表 B.8 C.5.14	HR	用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、范根（Fagan）检查法，设计复审
4	动态分析和测试	B.6.5 表 B.2	HR	用于所有新开发的代码
5	软件设计规范和软件验证（包括数据验证）计划之间的向前可追溯	C.2.11 C.5.14	HR	检查完整性：复审以确保所有的修改规程对于软件安全要求是足够的
6	软件验证（包括数据验证）计划和软件设计规范之间的向后可追溯	C.2.11	HR	最小化复杂性：复审以确保所有的修改规程是必要的
7	离线数值分析	C.2.13	HR	未使用。计算的数值稳定性在这儿不是一个关注的重点
	软件模块测试和集成	见本部分表 E.15		

表 E.19（续）

技术/措施	Ref.	SIL3	在本应用中的解释
可编程电子集成测试	见本部分表 E.16		
软件系统测试(确认)	见本部分表 E.17		
注：在参考栏(题头为 Ref.)，资料性的参考“B.x.x.x”，“C.x.x.x” 是指在 GBT 20438.7—2017 附录 B 和附录 C 中的技术描述，而“Table A.x”，“Table B.x”指的是在 GBT 20438.3—2017 附录 A 和附录 B 中的技术表格。			

表 E.20 功能安全评估

（见 GB/T 20438.3—2017 的 8）

技术/措施		Ref.	SIL3	在本应用中的解释
1	检查表	B.2.5	R	已使用
2	判定/真值表	C.6.1	R	有限使用
3	失效分析	表 B.4	HR	故障树分析被广泛地使用；因果图也被有限的使用。
4	多样化软件的共因失效分析(如实际使用了多样化软件)	C.6.3	HR	已使用
5	可靠性框图	C.6.4	R	已使用
6	本部分第 8 章要求和软件功能安全评估计划之间的向前可追溯	C.2.11	HR	检查功能安全评估覆盖的完整性
注：在参考栏(题头为 Ref.)，资料性的参考“B.x.x.x”，“C.x.x.x” 是指在 GB/T 20438.7—2017 附录 B 和附录 C 中的技术描述，而“Table A.x”，“Table B.x”指的是在 GB/T 20438.3—2017 附录 A 和附录 B 中的技术表格。				

参 考 文 献

[1] GB/T 21109(所有部分) 过程工业领域安全仪表系统的功能安全

[2] GB 28526 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全

[3] GB/T 12668.502 调速电气传动系统 第5-2部分:安全要求 功能

下列参考文献给出了评价失效概率(见附录B)的更多详情:

[4] IEC 61078:2006 Analysis techniques for dependability—Reliability block diagram and boolean methods.

[5] IEC 61165:2006 Application of Markov techniques

[6] BS 5760 Reliability of system equipment and components—Part 2: Guide to assessment of reliability

[7] D. J. SMITH, Reliability, maintainability and risk—Practical methods for engineers, Butterworth—Heinemann, 5th edition, 1997, ISBN 0-7506-3752-8.

[8] R. BILLINGTON and R. N. ALLAN, Reliability evaluation of engineering systems, Plenum, 1992, ISBN 0-306-44063-6.

[9] W. M. GOBLE, Evaluating control system reliability—Techniques and applications, Instrument Society of America, 1992, ISBN 1-55617-128-5.

计算诊断率(见附录C)的有用参考文献包括下列文献:

[10] Reliability Analysis Center (RAC), Failure Mode/Mechanism Distributions, 1991, Department of Defense, United States of America, PO Box 4700, 201 Mill Street, Rome, NY 13440-8200, Organization report number: FMD-91, NSN 7540-01-280-5500.

[11] ALLESSANDRO BIROLINI, Qualität und Zuverlassigkeit technischer Systeme, Theorie, Praxis, Management, Dritte Auflage, 1991, Springer-Verlag, Berlin Heidelberg New York, ISBN 3-540-54067-9, 3 Aufl., ISBN 0-387-54067-9 3 ed. (available in German only).

[12] MIL-HDBK-217F, Military Handbook Reliability prediction of electronic equipment, 2 December 1991, Department of Defense, United States of America.

以下参考文献提供了共因失效(见附录D)的有关信息:

[13] Health and Safety Executive Books, email hsebooks@prolog.uk.com.

[14] R. HUMPHREYS, A., PROC., Assigning a numerical value to the beta factor common-cause evaluation, Reliability 1987.

[15] UPM3.1, A pragmatic approach to dependent failures assessment for standard systems, AEA Technology, Report SRDA-R-13, ISBN 085 356 4337, 1996.

表E.3中引用了下列标准:

[16] GB/T 15969.3—2005 可编程序控制器 第3部分:编程语言

[17] ISA-TR84.00.02—2002 Parts 1-5, Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques Package.

[18] IEC 61025:2006 Fault tree analysis (FTA)

[19] IEC 62551 Analysis techniques for dependability—Petri Net technique10

[20] ANIELLO AMENDOLA, kluwer academic publisher, ISPRA 16-19 November 1987, Advanced seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, ISBN 0-7923-0268-0.

[21] CORWIN L. ATWOOD, The Binomial Failure Rate Common Cause Model, Technometrics

May 1986 Vol 28 n°2.

[22] A. ARNOLD, A. GRIFFAULT, G. POINT, AND A. RAUZY. The altarica language and its semantics. Fundamenta Informaticae, 34, pp.109—124, 2000.

[23] M. BOITEAU, Y. DUTUIT, A. RAUZY AND J.-P. SIGNORET, The AltaRica Data-Flow. Language in Use: Assessment of Production Availability of a MultiStates System, Reliability Engineering and System Safety, Elsevier, Vol. 91, pp 747—755.

[24] A. RAUZY. Mode automata and their compilation into fault trees. Reliability Engineering and System Safety, Elsevier 2002, Volume 78, Issue 1, pp 1—12.

[25] For PDS method; see<www.sintef.no/pds>; and further background material in: Hokstad, Per; Corneliussen, Kjell Source: Reliability Engineering and System Safety, v 83, n 1, p 111—120, January 2004.

[26] IEC 60601 (all parts) Medical electrical equipment

[27] GB/T 20438.1—2017 电气/电子/可编程电子安全相关系统的功能安全 第1部分:一般要求

[28] GB/T 20438.5—2017 电气/电子/可编程电子安全相关系统的功能安全 第5部分:确定安全完整性等级的方法示例

[29] GB/T 20438.7—2017 电气/电子/可编程电子安全相关系统的功能安全 第7部分:技术和措施概述

GB/T 20438.6—2017/IEC 61508-6:2010

GB/T 20438.6-2017

*

书号:155066·1-57856