ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.6—2006/IEC 61508-6:2000

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

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

(IEC 61508-6:2000,IDT)

2006-07-25 发布　　2007-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

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

GB/T 20438.6-2006

引　言

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

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

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

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

GB/T 20438

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

——针对飞速发展的技术，建立一个足够健壮而广泛的能满足今后发展需要的框架。

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

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

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

——采用了一种基于风险的方案来确定安全完整性等级要求。

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

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

这些系统运行在：

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

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

注：单一E/E/PE安全相关系统不一定是单通道结构。

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

目　次

前　言

GB/T 20438 由下列 7 部分构成：

——第 1 部分：一般要求；

——第 2 部分：电气/电子/可编程电子安全相关系统的要求；

——第 3 部分：软件要求；

——第 4 部分：定义和缩略语；

——第 5 部分：确定安全完整性等级的方法示例；

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

——第 7 部分：技术和措施概述。

本部分是 GB/T 20438 的第 6 部分。

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

附录 A、附录 B、附录 C、附录 D、附录 E 为资料性附录。

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

a) 将“IEC 61508”改为“GB/T 20438”。

b) “本国际标准”一词改为“本标准”。

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

d) 用小数点“.”代替原标准中作为小数点的逗号“,”。

本部分由中国机械工业联合会提出。

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

本部分由机械工业仪器仪表综合技术经济研究所负责起草。

本部分主要起草人：郑旭、冯晓升、梅恪、王莉、欧阳劲松等。

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

1　范围

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

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

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

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

——附录D阐述了将硬件共同原因失效率量化的方法论。

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

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

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

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

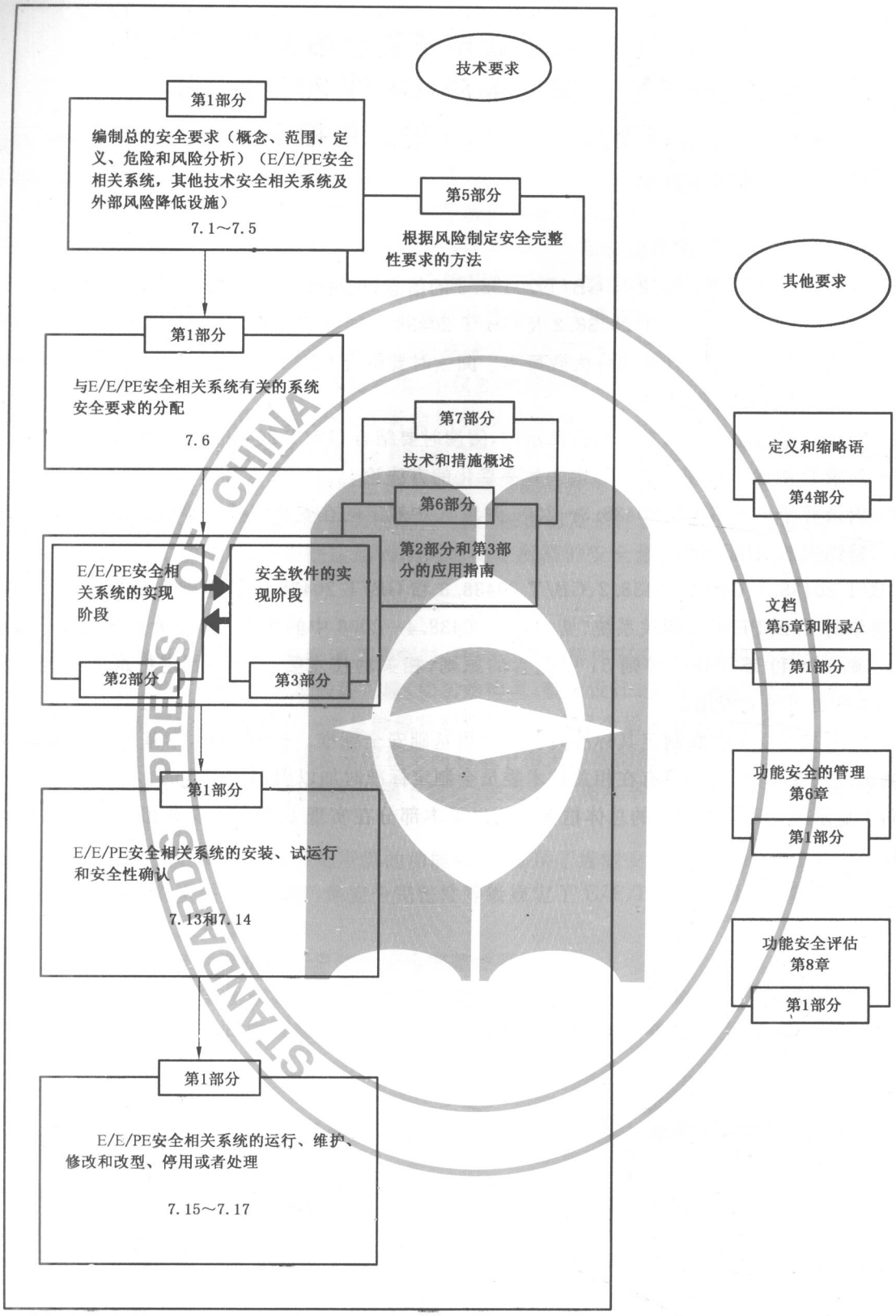


图 1　GB/T 20438 的总体框架

2 规范性引用文件

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

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

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

IEC/ISO 导则 51:1990 安全方面 在标准中引入安全条款的指南

3 定义和缩略语

见 GB/T 20438.4。

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

A.1 概述

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

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

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

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

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

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

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

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

——将在硬件及软件的规范、设计、修改中使用；并且

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

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

GB/T 20438.2 与 GB/T 20438.3 的要求包括：

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

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

---

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

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

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

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

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

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

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

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

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

——正确应用安全管理规程；

——任用合格的人员；

——应用规定的安全生命周期活动，包括规定的技术和措施[6]；

——一个独立的功能安全评估[7]。

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

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

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

A.2 GB/T 20438.2 应用中的功能步骤

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

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

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

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

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

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

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

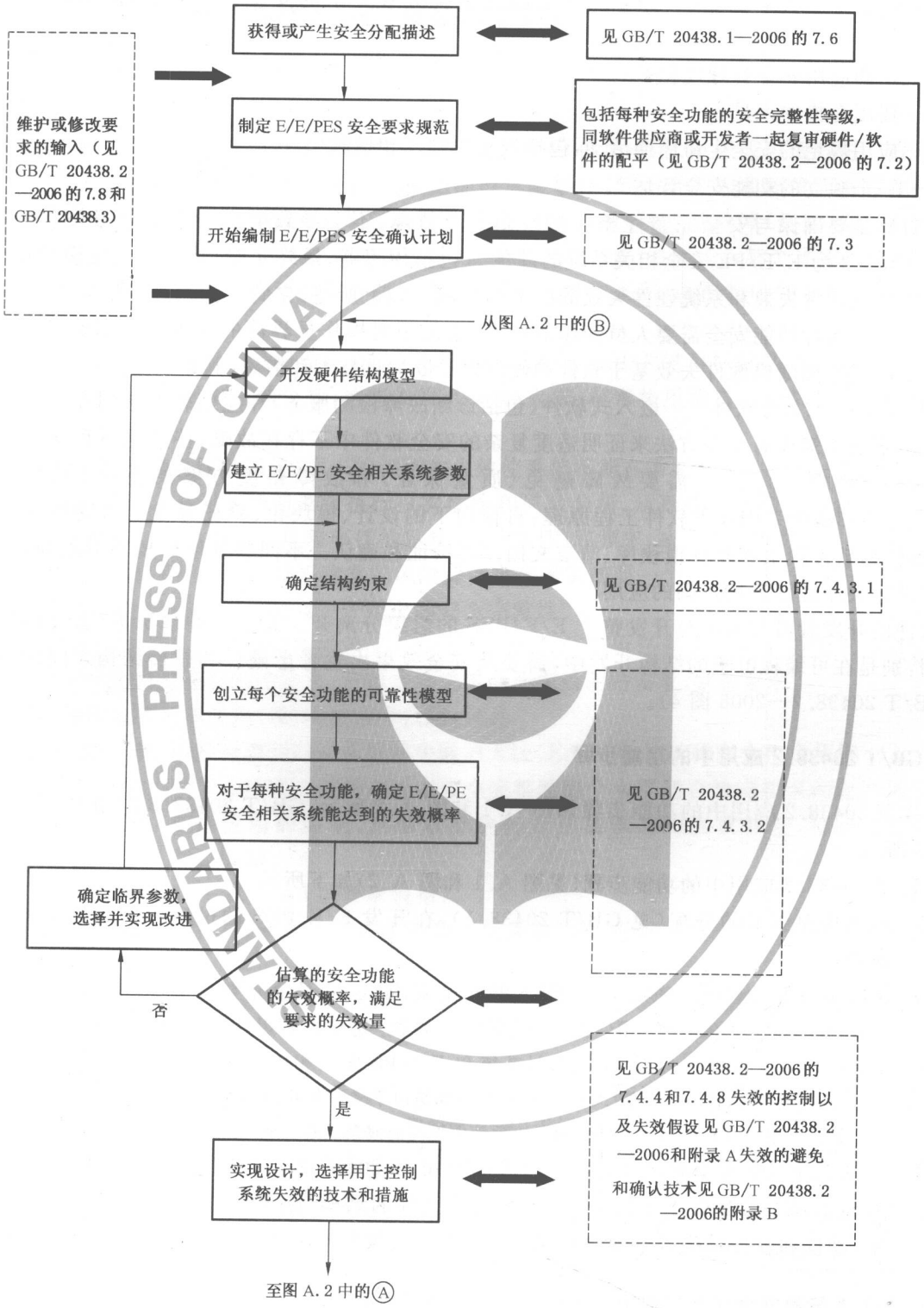
6) 如果在编制安全计划过程中合理性证明已文档化，GB/T 20438 中规定的那些措施可以被替代（见 GB/T 20438.1—2006 的第 6 章）。

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

8) 包括固定的内置软件或软件等效物（也称为固件），如专用集成电路。

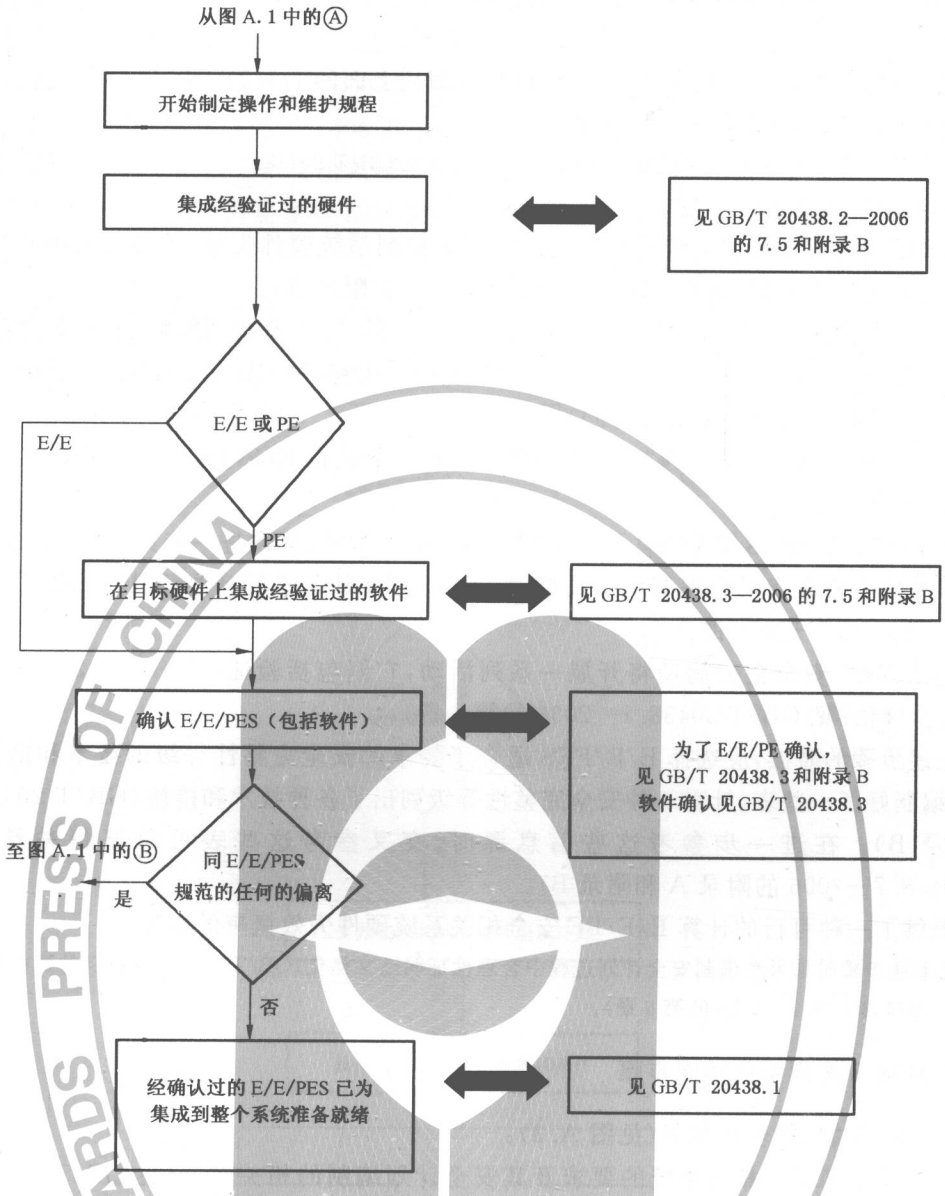
4)。如果需要将重复此步骤。

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



注：对于 PE 系统，针对软件的活动将并行发生(见图 A.3)。

图 A.1 GB/T 20438.2 的应用



注：对 PE 系统而言，软件的活动是并行的(见图 A.3)。

图 A.2　GB/T 20438.2 的应用

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

——失效的检验测试时间间隔，这些失效是不会自动被显现出来的；

——平均恢复时间；

——诊断覆盖率(见 GB/T 20438.2—2006 的附录 C)；

——失效概率；

——安全失效分数(见 GB/T 20438.2—2006 的附录 C)。

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

h) 创建 E/E/PE 安全相关系统需要执行的每个安全功能的可靠性模型。

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

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

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

——在可能时改变一个或多个子系统参数(返回到上面的 f))；和/或

——改变硬件结构(返回到上面的 d))。

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

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

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

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

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

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

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

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

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

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

A.3 GB/T 20438.3 应用中的功能步骤

GB/T 20438.3 的功能步骤如下(见图 A.3)：

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

注 1：早期生命周期阶段已经：

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

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

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

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

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

d) 开始编制软件安全验证和确认计划。

e) 根据以下条件设计、开发、验证或测试软件：

——软件安全计划编制；

——软件安全完整性等级；和

——软件安全生命周期。

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

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

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

h) 将软件安全确认的结果移交给系统工程师,以便进一步集成到整个系统中。

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

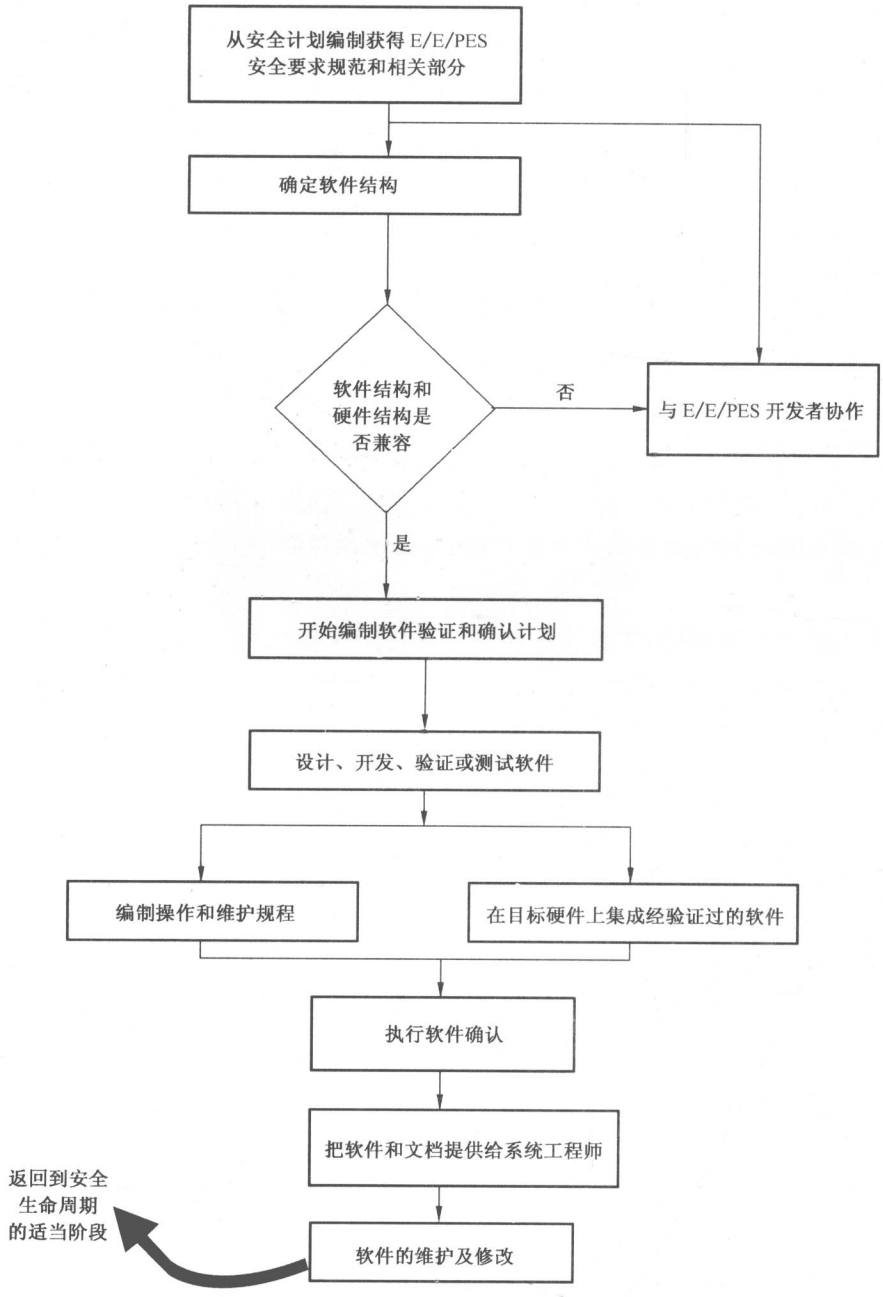


图 A.3 GB/T 20438.3 的应用

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

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

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

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

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

附 录 B
（资料性附录）
硬件失效概率评估技术示例

B.1 概述

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

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

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

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

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

计算基于以下假设：

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

——在系统寿命内部件失效概率为常量。

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

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

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

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

——在一个经表决过的组中所有通道具有相同的失效率和诊断覆盖率。

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

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