ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.2—2006/IEC 61508-2:2000

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

Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 2:Requirements for electrical/electronic/programmable electronic safety-related systems

(IEC 61508-2:2000,IDT)

2006-07-25 发布　　2007-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB/T 20438 由下列 7 部分构成：

——第 1 部分：一般要求；

——第 2 部分：电气/电子/可编程电子安全相关系统的要求；

——第 3 部分：软件要求；

——第 4 部分：定义和缩略语；

——第 5 部分：确定安全完整性等级的方法示例；

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

——第 7 部分：技术和措施概述。

本部分是 GB/T 20438 的第 2 部分。

本部分等同采用国际标准 IEC 61508-2:2000《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》(英文版)。

本部分的附录 A、附录 B、附录 C 为规范性附录。

本部分与 IEC 61508-2:2000 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 1.2 中的注 2，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：梅恪、冯晓升、王莉、郑旭、欧阳劲松等。

引　言

由电气和电子器件构成的系统，多年来在许多领域中执行其安全功能，以计算机为基础的系统（一般指可编程电子系统（PES））在许多领域中用于非安全目的，但也越来越多地用于安全目的，为使计算机系统技术更有效安全地使用，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，不仅要考虑各系统中元器件的问题（如传感器、控制器、执行器等），而且要考虑构成组合安全相关系统的所有安全相关系统。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生命周期的各阶段（如初始构思，整个设计、实现、运行和维护到停用）。

——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/PES 安全相关系统在不同领域中相关标准的制定，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。

——采用了一种可确定安全完整性等级要求的基于风险的方案。

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

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

这些系统运行在：

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

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

注：单一 E/E/PE 安全相关系统不一定是单通道结构。

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

电气/电子/可编程电子安全相关系统的功能安全 第2部分:电气/电子/可编程电子安全相关系统的要求

1 范围

1.1 GB/T 20438.2

a) 在使用前,应充分理解GB/T 20438.1,GB/T 20438.1提供了实现功能安全的总体结构框架。

b) 适用于GB/T 20438.1定义的安全相关系统,安全相关系统至少包含一种电气、电子或可编程电子基本部件。

c) 适用于E/E/PE安全相关系统中的所有子系统及其部件(包括传感器、执行器、操作员界面)。

d) 规定了如何按照GB/T 20438.1从整体安全要求中提取开发信息并将其分配到E/E/PE安全相关系统;规定了如何从整体安全要求中提取E/E/PES的安全功能要求和E/E/PES安全完整性要求。

e) 规定了在E/E/PE安全相关系统的设计和制造过程中所进行的活动的要求(例如:建立E/E/PES安全生命周期模型),软件除外,软件要求在GB/T 20438.3(见图2、图3)中给出;这些要求包含了用以避免和控制故障和失效发生的技术和措施的应用,并被划分成与安全完整性等级相对应的不同等级。

f) 规定了执行E/E/PE安全相关系统的安装、试运行以及最终安全确认所需的信息。

g) 不适用于E/E/PE安全相关系统的操作和维护阶段,这方面内容在GB/T 20438.1中给出。但是,本部分为用户提供了有关E/E/PE安全相关系统的操作和维护所需的信息和规程的准备要求。

h) 对E/E/PE安全相关系统进行各种修改的各方应满足的要求进行了规定。

注1:本部分直接面向供方和/或公司内部的工程部门,因此包含了对修改的要求。

注2:本部分与GB/T 20438.3的关系见图3。

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,尽管它们不适用于简单E/E/PE安全系统(见GB/T 20438.4—2006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,各技术委员会在起草标准时应考虑使用这些标准,因为技术委员会的责任之一是在起草自己的标准时凡是适用之处都应贯彻基础安全标准。GB/T 20438同时也可作为独立的标准使用。

在适用的情况下,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。

注:仅当所有相关要求得到满足时,才能达到E/E/PE安全相关系统的功能安全。因此,认真考虑和充分参照所有相关要求是十分重要的。

1.3 图1表示了GB/T 20438的总体框架,同时指出了本部分在达到E/E/PE安全相关系统的功能安全时所起的作用。GB/T 20438.6—2006的附录A详述了GB/T 20438.2和GB/T 20438.3的应用。

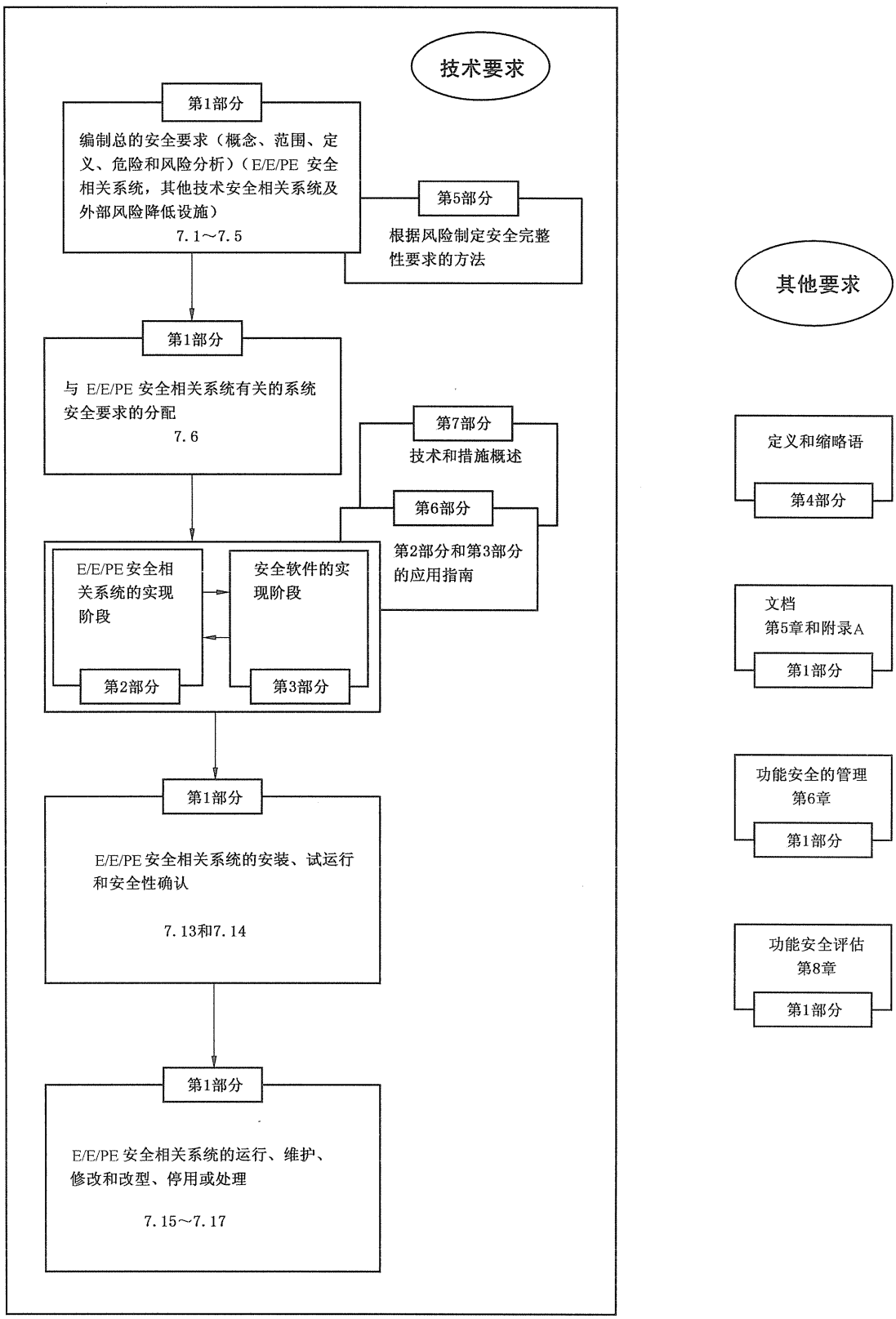


图 1 GB/T 20438 的总体框架

2 规范性引用文件

下列文件中的条款通过 GB/T 20438.2 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 20438.1—2006 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(IEC 61508-1:1998,IDT)

GB/T 20438.3—2006 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 61508-3:1998,IDT)

GB/T 20438.4—2006 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 61508-4:1998,IDT)

GB/T 20438.5—2006 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(IEC 61508-5:1998,IDT)

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(IEC 61508-6:2000,IDT)

GB/T 20438.7—2006 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(IEC 61508-7:2000,IDT)

IEC 60050(371):1984 国际电气词汇 371章：遥控

IEC 60300-3-2:1993 可靠性管理 第3部分：应用指南 第2篇：现场可靠性数据的采集

IEC 61000-1-1:1992 电磁兼容性(EMC) 第1部分：概述 第1篇：基本定义、术语的应用和说明

IEC 61000-2-5:1995 电磁兼容性(EMC) 第2部分：环境 第5篇：电磁环境的分类 基本电磁兼容性出版物

IEEE 352:1987 核电站安全相关系统可靠性分析一般原理的指南

ISO/IEC 导则 51:1990 安全方面 在标准中引入安全条款的指南

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

3 定义和缩略语

见 GB/T 20438.4。

4 与 GB/T 20438 的符合性

见 GB/T 20438.1—2006 的第4章。

5 文档

见 GB/T 20438.1—2006 的第5章。

6 功能安全管理

见 GB/T 20438.1—2006 的第6章。

7 E/E/PES 安全生命周期要求

7.1 一般要求

7.1.1 目的和要求：一般要求

7.1.1.1 本条阐述 E/E/PES 安全生命周期各阶段的目的和要求。

注：整体安全生命周期的目的和要求以及标准结构的简述在 GB/T 20438.1 中给出。

7.1.1.2 对于 E/E/PES 安全生命周期的所有阶段，表 1 给出了：

——需要达到的目的；

——各阶段的范围；

——要求所在的条款；

——各阶段所要求的输入；

——符合条款要求的输出。

7.1.2 **目的**

7.1.2.1 以系统化的方式构造应考虑的 E/E/PES 安全生命周期的各阶段，以达到 E/E/PE 安全相关系统所需的功能安全。

7.1.2.2 将贯穿于 E/E/PES 安全生命周期的有关 E/E/PE 安全相关系统功能安全的所有信息文档化。

7.1.3 **要求**

7.1.3.1 符合 GB/T 20438 的 E/E/PES 安全生命周期如图 2 所示。若应用其他安全生命周期，应在功能安全计划编制(见 GB/T 20438.1—2006 的第 6 章)时加以说明，并应满足本部分所有条款的目的和要求。

注：本部分和 GB/T 20438.3 的关系和范围见图 3。

7.1.3.2 功能安全的管理规程(见 GB/T 20438.1—2006 的第 6 章)应与 E/E/PES 安全生命周期的各阶段并行。

7.1.3.3 E/E/PES 安全生命周期的每个阶段都应根据各阶段规定的范围、输入、输出(见表 1)划分成相应的基本活动。

7.1.3.4 除非在功能安全的计划编制过程中有正当理由，否则 E/E/PES 安全生命周期的每个阶段的输出都应文档化(见 GB/T 20438.1—2006 的第 5 章)。

7.1.3.5 E/E/PES 安全生命周期的每个阶段的输出都应符合各阶段规定的目的和要求(见 7.2～7.9)。

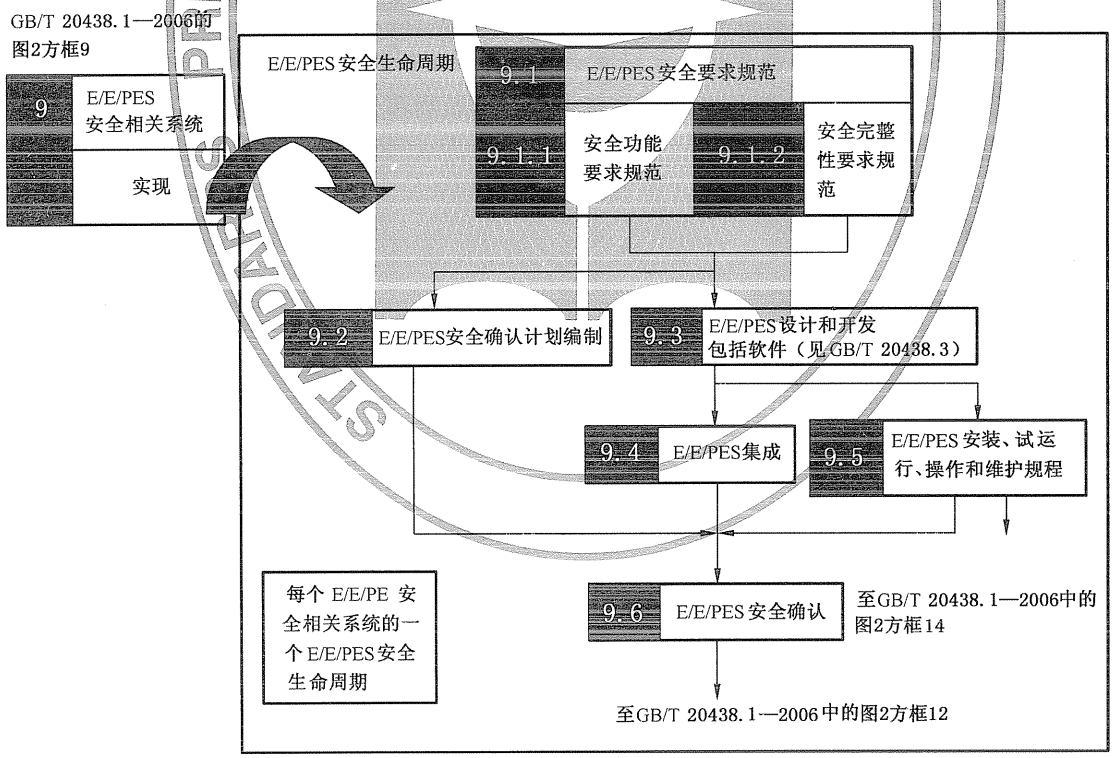


图 2 E/E/PES 安全生命周期(实现阶段)

注：另见 GB/T 20438.6—2006 附录 A 中的 A.2 b)。

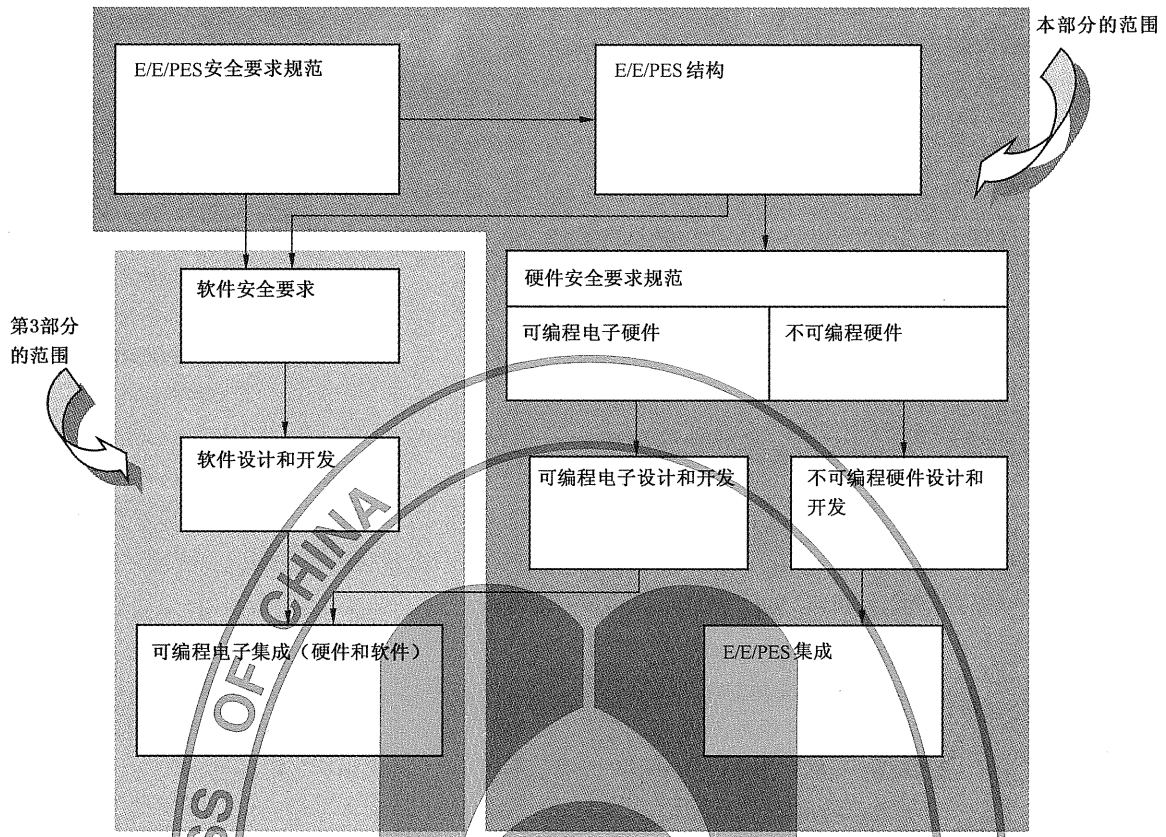


图 3　GB/T 20438.2 和 GB/T 20438.3 的范围和关系

表 1　E/E/PES 安全生命周期实现阶段概述

安全生命周期阶段或活动		目的	范围	要求所在的条款	输入	输出
图 2 中的方框号	标题					
9.1	E/E/PES 安全要求规范	为达到所需的功能安全，根据所需的安全功能和所需的安全完整性规定每个 E/E/PE 安全相关系统的要求	E/E/PE 安全相关系统	7.2.2	安全要求分配的描述（见 GB/T 20438.1—2006 的 7.6）	E/E/PES 安全要求； 软件安全要求（作为软件安全要求规范的输入）
9.2	E/E/PES 安全确认计划编制	编制 E/E/PE 安全相关系统的安全确认计划	E/E/PE 安全相关系统	7.3.2	E/E/PES 安全要求	E/E/PE 安全相关系统的安全确认计划
9.3	E/E/PES 设计和开发	设计满足安全功能要求和安全完整性要求的 E/E/PE 安全相关系统	E/E/PE 安全相关系统	7.4.2～7.4.8	E/E/PES 安全要求	符合 E/E/PES 安全要求的 E/E/PE 安全相关系统设计； E/E/PES 集成测试计划； PES 结构化信息（作为软件要求规范的输入）

表 1(续)

安全生命周期阶段或活动		目的	范围	要求所在的条款	输入	输出
图 2 中的方框号	标题					
9.4	E/E/PES 集成	集成和测试 E/E/PE 安全相关系统	E/E/PE 安全相关系统	7.5.2	E/E/PES 设计； E/E/PES 集成测试计划； 可编程电子硬件和软件	符合 E/E/PES 设计的全功能的 E/E/PE 安全相关系统； E/E/PES 集成测试的结果
9.5	E/E/PES 安装、试运行、操作和维护规程	制定规程以保证 E/E/PE 安全相关系统在操作和维护期间保持功能安全	E/E/PE 安全相关系统； EUC	7.6.2	E/E/PES 安全要求； E/E/PES 设计	各个 E/E/PES 单独安装、试运行、操作和维护的规程
9.6	E/E/PES 安全确认	在所有方面，确认 E/E/PE 安全相关系统满足基于所需安全功能和所需安全完整性的安全要求	E/E/PE 安全相关系统	7.7.2	E/E/PES 安全要求； E/E/PE 安全相关系统的安全确认计划	经充分安全确认的 E/E/PE 安全相关系统； E/E/PES 安全确认结果
—	E/E/PES 修改	改正、加固或适应 E/E/PE 安全相关系统，以保证达到和维持所需的安全完整性等级	E/E/PE 安全相关系统	7.8.2	E/E/PES 安全要求	E/E/PES 修改结果
—	E/E/PES 验证	就某阶段输入的产品和标准而言，测试和评价该阶段的输出，以保证正确性和一致性	E/E/PE 安全相关系统	7.9.2	同上，依赖于某阶段； 每个阶段 E/E/PE 安全相关系统的验证计划	同上，依赖于某阶段； 每个阶段 E/E/PE 安全相关系统的验证结果
—	E/E/PES 功能安全评估	调查和判断 E/E/PE 安全相关系统所达到的功能安全	E/E/PE 安全相关系统	8	E/E/PES 功能安全评估计划	E/E/PES 功能安全评估结果

7.2 E/E/PES 安全要求规范

注：这一阶段是图 2 的方框 9.1。

7.2.1 目的

为达到所需的功能安全，根据所需的安全功能和所需的安全完整性规定每个 E/E/PE 安全相关系统的要求。

注：例如，要使 EUC 进入安全状态或保持安全状态要对安全功能提出要求。

7.2.2 一般要求

7.2.2.1 E/E/PES 安全要求规范应来源于 GB/T 20438.1—2006 的 7.6 规定的安全要求的分配，以及功能安全计划编制中规定的要求(见 GB/T 20438.1—2006 的第 6 章)。E/E/PES 的开发者应可获得这些信息。

注：如果同一 E/E/PE 安全相关系统即执行非安全功能又执行安全功能，要加倍谨慎。虽然，这是标准所允许的，

但这将会导致执行 E/E/PE 安全生命周期活动(例如设计、确认、功能安全评估和维护)的过程更加复杂并使难度增加。

7.2.2.2 E/E/PES 的安全要求应按以下要求表述和组织

a) 清晰、准确、无歧义、可验证、可测试、可维护并切实可行;和

b) 便于采用 E/E/PES 安全生命周期任一阶段信息的各方理解。

7.2.2.3 E/E/PES 安全要求规范应包含 E/E/PES 安全功能要求(见 7.2.3.1)和 E/E/PES 安全完整性要求(见 7.2.3.2)。

7.2.3 E/E/PES 安全要求

7.2.3.1 E/E/PES 安全功能要求规范应包括:

a) 达到要求功能安全所需的所有安全功能的描述,针对每一安全功能应:

——为 E/E/PE 安全相关系统的设计与开发提供充分的、可理解的详细要求;

——包括一种方式,在这种方式下,E/E/PE 安全相关系统被用来达到或保持 EUC 的某种安全状态;

——规定在达到或保持 EUC 安全状态时是否要求连续控制,以及在什么时期控制;

——规定在低要求操作模式下,高要求或连续操作模式下,安全功能是否适用于 E/E/PE 安全相关系统。

b) 吞吐量与响应时间指标。

c) 为达到要求的功能安全,所必需的 E/E/PE 安全相关系统和操作员界面。

d) 与安全功能相关的会对 E/E/PE 安全相关系统的设计产生影响的所有信息。

e) E/E/PE 安全相关系统与其他系统之间的所有接口(与 EUC 直接关联的外部接口或内部接口)。

f) EUC 操作的所有相关模式,包括:

——使用准备,包括设置与调整;

——启动、教学、全自动、手动、半自动、稳定的工作状态;

——非工作时的稳定状态,重设置,关机,维护;

——合理的、可预见的异常工况。

注 1:合理的、可预见的异常工况是指开发者与用户所能合理预见到的异常工况。

注 2:特殊的操作模式(例如设置、调整、维护)可能要求附加的安全功能,以使这些操作能安全执行。

g) E/E/PE 安全相关系统行为的所有要求模式——尤其是 E/E/PE 安全相关系统的失效行为和要求的响应(例如报警、自动关机等)应当详细说明。

h) 所有硬件或软件相互作用的重要性——当相关时,硬件或软件之间要求的约束应加以标识和文档化。

注 3:在完成设计之前不知道相互作用的情况下,只能对一般约束加以说明。

i) E/E/PE 安全相关系统和相关子系统的限制与约束条件,例如:定时约束。

j) 启动和再启动 E/E/PE 安全相关系统的有关规程的任何特殊要求。

7.2.3.2 E/E/PES 安全完整性要求规范应包括:

a) 每一安全功能的安全完整性等级,以及需要时(见注 2)安全功能要求的目标失效量。

注 1:依照 GB/T 20438.1—2006 的表 2 和表 3,某个安全功能的安全完整性等级确定了该安全功能的目标失效量。

注 2:在使用定量方法推导安全功能所需的风险降低时,需要规定该安全功能的目标失效量(见 GB/T 20438.1—2006 的 7.5.2.2)。

b) 每一安全功能的操作模式(低要求、高要求或连续)。

c) 使 E/E/PE 的硬件检验测试得以实施的要求、约束、功能与设备。

d) 在 E/E/PES 的安全生命周期中,包括制造、贮存、运输、检测、安装、试运行、操作和维护中可

能遇到的极端环境条件。

e) 达到的电磁兼容性要求的抗电磁干扰极限(见 IEC 61000-1-1)——抗电磁干扰极限,应依据电磁环境(见 IEC 61000-2-5)和所需的安全完整性等级得出。

注 1:认识到安全完整性等级是决定抗电磁干扰极限的一个因素是很重要的,特别是由于环境的电磁干扰水平服从统计分布的原因。在很多现实情况下,不可能规定一个绝对的干扰水平。实际上,只能预计不超过某一水平(就是电磁兼容水平)。但是操作中的困难使得这种预计的概率难以确定。因此,抗干扰极限并不能保证 E/E/PE 安全相关系统不会由于电磁干扰而失效,它仅为在某种程度上提供某种置信度水平。实际达到的置信度水平是在操作环境下与干扰水平的统计分布有关的抗干扰极限功能。安全完整性等级越高就需要更高的置信度水平,这意味着对于越高的安全完整性等级,抗干扰极限超过电磁兼容水平的容限应当越大。

注 2:同时,在 EMC 产品标准中可以找到相应的指导,但重要的是要认识到如果设备要在严酷的电磁环境下使用或装在某些特殊的位置时,抗干扰水平要高于这些标准中规定的水平。

注 3:在拟定 E/E/PES 安全要求规范时,要考虑 E/E/PE 安全相关系统的应用领域。这对维护尤其重要,规定的检验测试间隔要不小于对特殊应用的合理预期值。例如,公众使用的批量生产项目中实际得到的服务间隔时间要比在有更多控制的应用中的服务间隔时间大得多。

7.2.3.3 为避免 E/E/PES 安全要求规范中的失误,应当使用表 B.1 中的一组合适的技术和措施。

7.3 E/E/PES 安全确认计划编制

注:这一阶段是图 2 的方框 9.2。它通常与 E/E/PES 设计和开发并行(见 7.4)。

7.3.1 目的

编制 E/E/PE 安全相关系统的安全确认计划。

7.3.2 要求

7.3.2.1 编制计划以便规定用于证明 E/E/PE 安全相关系统满足 E/E/PES 安全要求规范(见 7.2)的步骤(包括规程的和技术的)。

注:见 GB/T 20438.3 的软件确认计划。

7.3.2.2 编制 E/E/PE 安全相关系统的确认计划应考虑:

a) E/E/PES 安全要求规范定义的所有要求;

b) 用于确认每一安全功能正确实现的规程和在完成测试时的通过或未通过的准则;

c) 用于确认每一安全功能所需的安全完整性的规程和在完成测试时通过或未通过的准则;

d) 测试所需的环境,包括所有所需的工具和设备(还包括工具与设备的校准计划);

e) 测试评价规程(带合理性证明);

f) 应用于确认规定的抗电磁干扰极限的测试规程和性能准则;

注:抗干扰测试极限规范的指南由 IEC 61000-2-5 和 IEC 61000-4 给出。

g) 解决确认失效的方针。

7.4 E/E/PES 的设计与开发

注:这一阶段是图 2 的方框 9.3,它通常与 E/E/PES 安全确认计划编制并行(见 7.3)。

7.4.1 目的

确保 E/E/PE 安全相关系统的设计和实现满足规定的安全功能和安全完整性要求(见 7.2)。

7.4.2 一般要求

7.4.2.1 考虑 7.4 的所有要求,并根据 E/E/PES 安全要求规范(见 7.2)设计 E/E/PE 安全相关系统。

7.4.2.2 E/E/PE 安全相关系统的设计(包括硬、软件的整体结构、传感器、执行器、可编程电子、嵌入式软件和应用软件等,见图 4),应当符合以下 a)~c)的全部要求:

a) 硬件安全完整性要求包括:

——硬件安全完整性的结构约束(见 7.4.3.1);和

——危险随机硬件失效概率的要求(见 7.4.3.2)。

b) 系统安全完整性要求包括：

——避免失效的要求(见 7.4.4)和系统故障控制的要求(见 7.4.5)；或

——设备“经使用证实”的证据(见 7.4.7.6～7.4.7.12)。

c) 故障检测时对系统行为的要求(见 7.4.6)。

注 1：E/E/PES 安全完整性整体框架：为证明达到 E/E/PE 安全相关系统中的某个安全完整性等级(硬件的和系统的)，选择一种设计方案的总体方法如下：

——确定安全功能所要求的安全完整性等级(SIL)(见 GB/T 20438.1 和 GB/T 20438.5)；

——设置：硬件安全完整性＝系统安全完整性＝SIL(见 7.4.3.2.1)；

——对于硬件安全完整性，确定能够满足结构约束条件的结构(见 7.4.3.1)，并且证明由于随机硬件失效引起的安全功能失效的概率能够满足要求的目标失效量(见 7.4.3.2)；

——对于系统安全完整性，选择实际操作中控制(容许)系统故障(见 7.4.5)的设计特性或是证明“经使用证实”的要求已经得到满足(见 7.4.7.6～7.4.7.12)；

——对于系统安全完整性，选择在设计与开发中避免(防止引入)系统故障(见 7.4.4)的技术和措施或是证明“经使用证实”的要求已经得到满足(见 7.4.7.6～7.4.7.12)。

注 2：GB/T 20438.3 包括软件结构要求(见 7.4.2.2)；产生可编程电子和软件集成测试规范的要求(见 7.5)；依据该规范(见 7.5)集成可编程电子和软件的要求。在所有情况下，E/E/PE 安全相关系统的开发者与软件开发者之间的密切合作都是必需的。

结构示例，可以是：

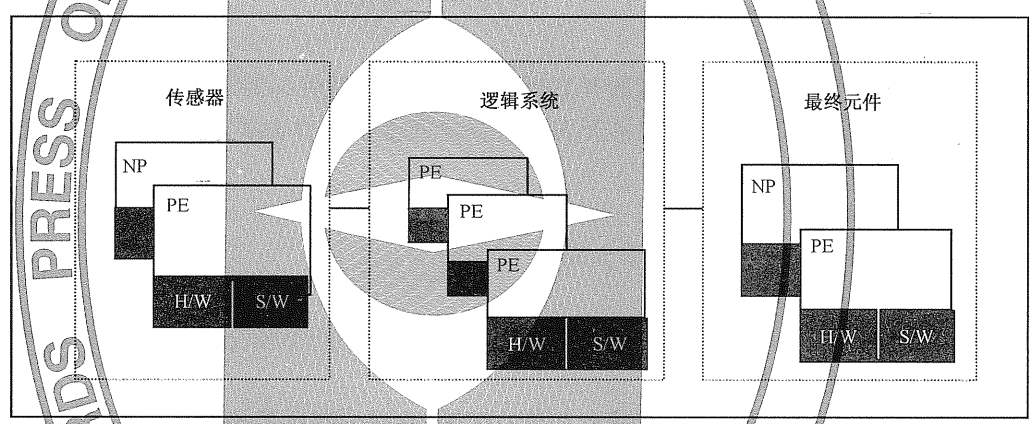
——单通道；

——双通道；

——1oo2，

1oo3，

2oo2 等



可编程电子结构		
PE 硬件结构	**PE 软件结构(S/W 结构包括嵌入式 S/W 和应用 S/W)**	
PE 硬件中通用的和应用时的具体特性： 例如包括： ——诊断测试； ——冗余处理器； ——双 I/O 卡	PE 嵌入式软件	PE 应用软件
	例如包括： ——通信驱动器； ——故障处理； ——可执行软件	例如包括： ——输入/输出功能； ——派生功能(例如，未提供嵌入式软件服务时的传感器检验)

关键词：

PE：可编程电子

NP：非可编程装置

H/W：硬件

S/W：软件

MooN：N 中的 M(如 1oo2 为 2 中的 1)

图 4 可编程电子中软件结构和硬件结构的关系

7.4.2.3 在E/E/PE安全相关系统既执行安全功能又执行非安全功能的地方，除非能够表明实现安全功能和非安全功能是充分独立的(也就是说，非安全功能的失效不会引起安全功能的危险失效)，否则所有的软硬件都应被视为与安全相关的。只要可行，安全功能应与非安全功能分开。

注1：非安全和安全部件之间相关失效概率与安全功能包含的最高安全完整性等级相比足够低，即意味着实现的充分独立。

注2：当在同一E/E/PE安全相关系统中实现非安全功能和安全功能时，要谨慎操作。虽然，这是标准所允许的，但这将会导致执行E/E/PE安全生命周期活动(例如设计、确认、功能安全评估和维护)的过程更加复杂并使难度增加。

7.4.2.4 软硬件的要求由拥有最高安全完整性等级的安全功能的安全完整性等级来决定，除非能够表明不同安全完整性等级的安全功能的实现是充分独立的。

注1：实现不同安全完整性等级的安全功能的各部分之间的相关失效概率与安全功能包含的最高安全完整性等级相比足够低，即意味着实现的充分独立。

注2：在一个E/E/PE安全相关系统实现几个安全功能时，需要考虑单一故障会引起几个安全功能失效的概率。在这种情况下，恰当的作法是根据这类失效的风险，按照比任何一个安全功能相关的安全完整性等级更高的安全完整性等级确定软硬件的要求。

7.4.2.5 在要求安全功能之间相互独立(见7.4.2.3和7.4.2.4)时，在设计时以下几条应文档化：

a) 达到独立的方法；

b) 方法的合理性证明。

7.4.2.6 E/E/PE安全相关系统的开发者应可获得安全软件的要求(见GB/T 20438.3)。

7.4.2.7 E/E/PE安全相关系统的开发者应复审安全软硬件的要求，以保证其已充分规定。E/E/PE的开发者应特别考虑：

a) 安全功能；

b) E/E/PE安全相关系统安全完整性要求；

c) 设备与操作员界面。

7.4.2.8 E/E/PE安全相关系统设计文档应规定在E/E/PES安全生命周期各阶段中为达到安全完整性等级所必需的技术和措施。

7.4.2.9 E/E/PE安全相关系统设计文档应证明，为形成满足要求的安全完整性等级的集成集所选择的技术和措施的合理性。

注：E/E/PE安全相关系统(包括传感器、执行器等)采用独立类型的软硬件、诊断测试和编程工具，并利用适当的软件语言，都有可以降低E/E/PES应用工程的复杂性的潜力。

7.4.2.10 在设计与开发活动中，应认识、评估和文档化所有软硬件相互作用的重要意义(如相关)。

7.4.2.11 设计应基于子系统分解的方法，每一个子系统有规定的设计和系列集成测试(见7.4.7)。

注1：一个部件或任意部件组都可以认为是一个子系统。一个完整的E/E/PE安全相关系统是由一系列一起执行安全功能的、可识别并分开的子系统构成。子系统可以拥有一个以上的通道，见7.4.7.3。

注2：只要可行，在实现中要尽量使用现有的经验证过的子系统。本陈述一般仅在下述两种情况下有效：如果现有子系统的功能、能力、性能几乎能够100%地映射于新要求上；或是已验证过的子系统由这样一种方式组成，即用户仅能选择特殊应用所需的功能、能力和性能。如果现有子系统被做得太复杂或是有未被使用的特性，并且不能防止不期望的功能，过多的功能、能力或性能会有损于系统安全。

7.4.2.12 带多路输出的子系统，有必要确定由E/E/PE安全相关系统失效引起的一些输出状态的组合是否能够直接引发危险事件(如用危险与风险分析来确定，见GB/T 20438.1—2006的7.4.2.10)。本条建立后，对输出状态的组合的预防措施应被视为在高要求或连续操作模式下工作的一个安全功能(见7.4.6.3和7.4.3.2.5)。

7.4.2.13 所有的部件应尽可能降额(见GB/T 20438.7—2006附录A的A.2.8)使用。在其极限值下使用任意部件的合理性证明应文档化(见GB/T 20438.1—2006的第5章)。

注：降额系数至少为0.67才合适。

7.4.3 硬件安全完整性要求

注：GB/T 20438.6—2006 附录 A 的 A.2 提供了达到要求的硬件安全完整性所需步骤的概述，并说明了本条与 GB/T 20438 的其他要求之间的关系。

7.4.3.1 硬件安全完整性的结构约束

7.4.3.1.1 硬件安全完整性的安全功能所声明的最高安全完整性等级，受限于硬件故障裕度和执行该安全功能的子系统的安全失效分数(见附录 C)。表 2 和表 3 规定了安全功能所声明的最高安全完整性等级，该安全功能使用了一个考虑了该子系统的硬件故障裕度和安全失效分数的子系统(见附录 C)。表 2 与表 3 的要求应适用于执行安全功能的每一子系统和 E/E/PE 安全相关系统的每一部分。7.4.3.1.2～7.4.3.1.4 规定了表 2 与表 3 中的哪一个适用于任一特定子系统。7.4.3.1.5 和 7.4.3.1.6 规定了如何导出安全功能所声明的最高安全完整性等级。对于这些要求：

a) 硬件故障裕度 N 意味着 $N+1$ 个故障会导致全功能的丧失，在确定硬件故障裕度时不考虑其他可能控制故障影响的措施，如诊断。

b) 若一个故障可直接引起一个或几个后续故障的发生，这些故障可视为单个故障。

c) 在确定硬件故障裕度时，如果相对于子系统安全完整性而言某些故障出现的可能性很小，这些故障可不考虑。不考虑这类故障的合理性应被证明和文档化(见注 3)。

d) 子系统安全失效分数的定义为子系统的平均安全失效率加检测到的平均危险失效率与子系统总平均失效率之比(见附录 C)。

注 1：为了达到足够健壮的结构，考虑到子系统的复杂水平，已经包括了结构的约束。通过应用这些要求得到的 E/E/PE 安全相关系统的硬件安全完整性等级是允许声明的最高值。尽管在某些情况下，如果对 E/E/PE 安全相关系统采用纯数学方法，在理论上也可以导出更高的安全完整性等级。

注 2：为满足硬件故障裕度要求而导出的结构和子系统是在正常操作条件下使用的。当 E/E/PE 安全相关系统进行在线修理时，故障裕度要求可适当放宽。但是，与放宽要求相关的关键参数必须进行事先评价(例如：平均恢复时间与一次要求的概率作比较)。

注 3：如果一个部件由于设计与结构(例如，一个机械执行器连接器)的固有属性的特点仅具有极小的失效概率，将不必考虑使用该部件时任何安全功能的安全完整性所需的约束(基于硬件故障裕度)。

7.4.3.1.2 满足下列条件，其部件被要求达到安全功能的一个子系统可视为 A 类：

a) 所有组成部件的失效模式都被很好地定义；并且

b) 故障状况下子系统的行为能够完全确定；并且

c) 通过现场经验获得充足而可靠的数据，可显示出满足所声明的检测到的和未检测到的危险失效的失效率(见 7.4.7.3 和 7.4.7.4)。

7.4.3.1.3 满足下列条件，其部件被要求达到安全功能的一个子系统可视为 B 类：

a) 至少一个组成部件的失效模式未被很好地定义；或

b) 故障状况下子系统的行为不能完全确定；或

c) 通过现场经验获得的可靠的数据不够充分，不足以显示出满足所声明的检测到的和未检测到的危险失效的失效率(见 7.4.7.3 和 7.4.7.4)。

注：这就是说，如果子系统中只要有一个组成部件满足 B 类的条件，那么这个子系统应被视为 B 类，而不是 A 类。参见 7.4.2.11 的注 1。

7.4.3.1.4 表 2 或表 3 的结构约束应适用于每一个执行安全功能的子系统，所以：

a) 应达到整个 E/E/PE 安全相关系统的硬件故障裕度的要求；

b) 表 2 用于 E/E/PE 安全相关系统构成中的每一个 A 类子系统；

注 1：如果 E/E/PE 安全相关系统仅包括 A 类子系统，那么在表 2 中的要求将适用于整个 E/E/PE 安全相关系统。

c) 表 3 用于 E/E/PE 安全相关系统构成中的每一个 B 类子系统；

注 2：如果 E/E/PE 安全相关系统仅包括 B 类子系统，那么在表 3 中的要求将适用于整个 E/E/PE 安全相关系统。

d) 表 2 与表 3 适用于由 A 类和 B 类子系统组成的 E/E/PE 安全相关系统，表 2 的要求适用于 A 类子系统，表 3 的要求适用于 B 类子系统。

表 2　硬件安全完整性:A 类安全相关子系统的结构约束

安全失效分数	硬件故障裕度(见注 2)		
	0	1	2
<60%	SIL1	SIL2	SIL3
60%～<90%	SIL2	SIL3	SIL4
90%～<99%	SIL3	SIL4	SIL4
≥ 99%	SIL3	SIL4	SIL4

注 1：本表的详细解释见 7.4.3.1.1～7.4.3.1.4。

注 2：硬件故障裕度 N 表示 $N+1$ 个故障将导致安全功能的丧失。

注 3：如何计算安全失效分数见附录 C。

表 3　硬件安全完整性:B 类安全相关子系统的结构约束

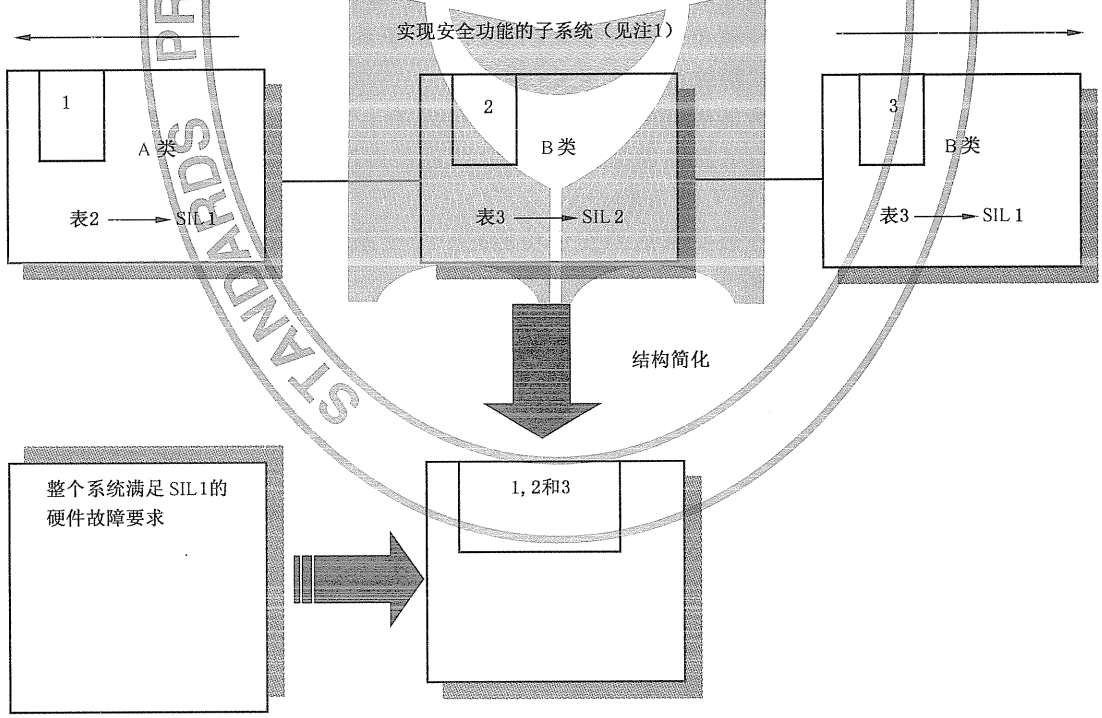
安全失效分数	硬件故障裕度(见注 2)		
	0	1	2
<60%	不允许	SIL1	SIL2
60%～<90%	SIL1	SIL2	SIL3
90%～<99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

注 1：本表的详细解释见 7.4.3.1.1～7.4.3.1.4。

注 2：硬件故障裕度 N 表示 $N+1$ 个故障将导致安全功能的丧失。

注 3：如何计算安全失效分数见附录 C。

7.4.3.1.5　在 E/E/PE 安全相关系统中,若某安全功能是通过单一通道实现的(见图 5),该安全功能所能声明的最大硬件安全完整性等级取决于能满足最低硬件安全完整性等级要求的子系统(由表 2 与表 3 确定)。



注 1：子系统实现安全功能要贯穿从传感器到执行器的整个 E/E/PE 安全相关系统。

注 2：充分理解本图,详见 7.4.3.1.5 的示例。

图 5　单通道安全功能的硬件安全完整性限制示例

示例：假设某结构中的一个特殊安全功能通过子系统1、2、3的单一通道实现，如图5所示，而子系统满足表2、表3中的如下要求：

——子系统1达到SIL1的硬件故障裕度要求，对应一个特定安全失效分数；

——子系统2达到SIL2的硬件故障裕度要求，对应一个特定安全失效分数；

——子系统3达到SIL1的硬件故障裕度要求，对应一个特定安全失效分数。

对于此特定结构，子系统1和3仅能达到SIL1的硬件故障裕度要求，同时子系统2能达到SIL2的硬件故障裕度要求。因此，对于所考虑的安全功能的硬件故障裕度，子系统1和3把所要声明的硬件安全完整性等级，限制为只能是SIL1。

7.4.3.1.6 在E/E/PE安全相关系统中，若某个安全功能是通过其子系统的多个通道实现的（如图6），该安全功能所能声明的最大硬件安全完整性等级取决于：

a) 根据表2或表3的要求评估每一子系统（详见7.4.3.1.2～7.4.3.1.4）；并且

b) 将子系统组成为组合；并且

c) 分析这些组合以确定整体硬件安全完整性等级。

示例：这些组合的组成和分析有多种方法。为了举例说明一种可能的方法，假设某结构中的一个特殊安全功能可通过子系统1、2和3组合实现，还可通过子系统4、5和3组合实现，如图6所示。在此情况下，子系统1、2的组合与子系统4、5的组合对于安全功能来讲有相同的功能性，并且提供独立的输入到子系统3。在这个例子中，并联子系统的组合是基于每一子系统实现所需的安全功能部分不依赖于其他子系统（并联）。出现如下情况，也可实现安全功能：

——子系统1或2出现故障（由于子系统4和5的组合能够实现安全功能）；

——子系统4或5出现故障（由于子系统1和2的组合能够实现安全功能）。

每一子系统满足表2与表3的要求如下：

——子系统1达到SIL3的硬件故障裕度要求，对应一个特定安全失效分数；

——子系统2达到SIL2的硬件故障裕度要求，对应一个特定安全失效分数；

——子系统3达到SIL2的硬件故障裕度要求，对应一个特定安全失效分数；

——子系统4达到SIL2的硬件故障裕度要求，对应一个特定安全失效分数；

——子系统5达到SIL1的硬件故障裕度要求，对应一个特定安全失效分数。

在确定所考虑的安全功能所能声明的最高硬件安全完整性等级时，应按照如下详细步骤：

a) 组合子系统1和2：子系统1和2的组合所能达到的硬件故障裕度和安全失效分数（每一子系统分别满足SIL3和SIL2的要求）满足SIL2的要求（由子系统2确定）。

b) 组合子系统4和5：子系统4和5的组合所能达到的硬件故障裕度和安全失效分数（每一子系统分别满足SIL2和SIL1的要求）满足SIL1的要求（由子系统5确定）。

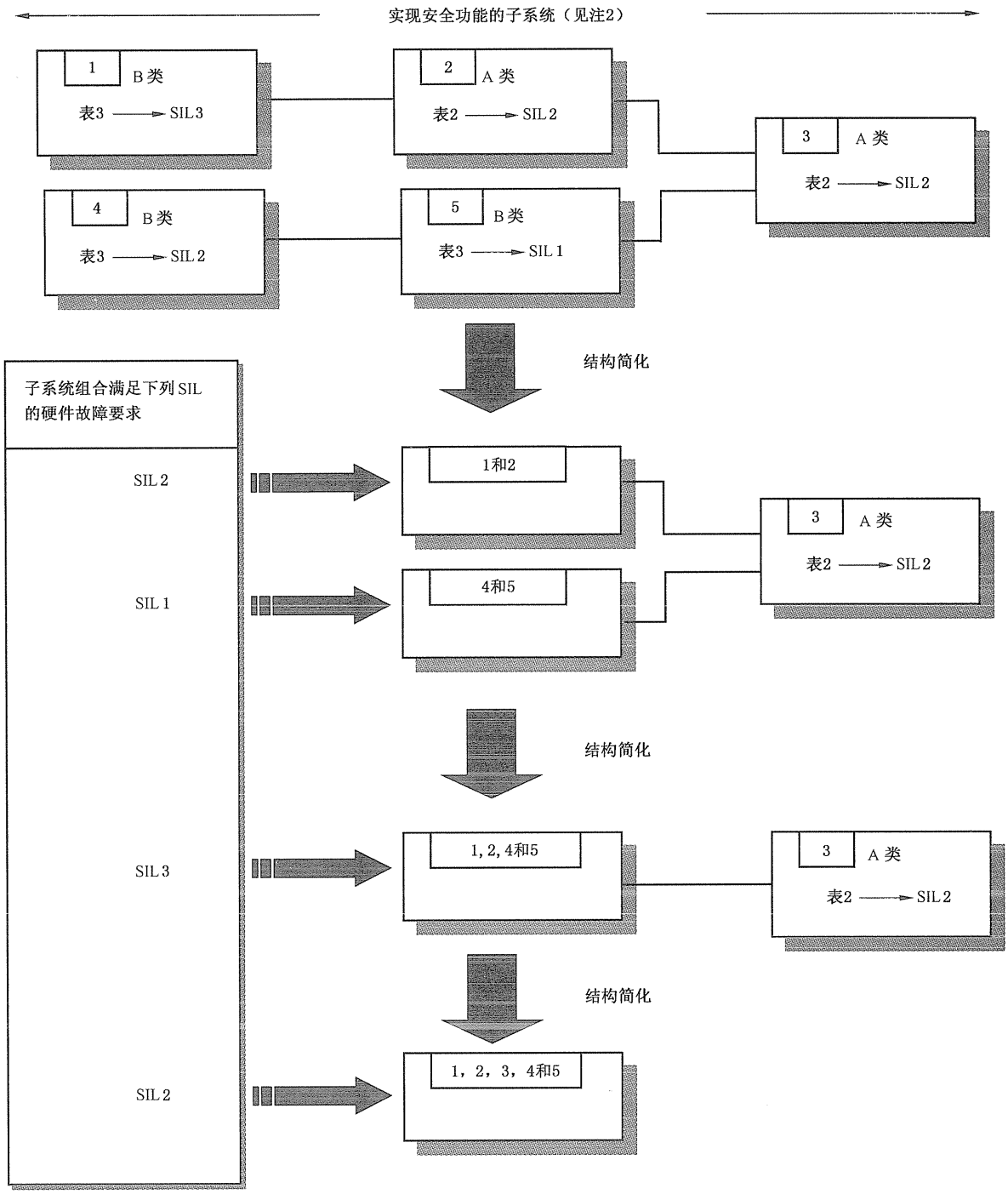
c) 进而将子系统1和2的组合与子系统4和5的组合进行组合：根据硬件故障裕度，子系统1、2、4和5的组合的硬件安全完整性等级由以下决定：

——决定哪种子系统的组合（也就是子系统1和2的组合或子系统4和5的组合）已达到最高可声明的硬件安全完整性等级（基于满足硬件故障裕度）；

——分析其他子系统的组合对子系统1、2、4、5组合的硬件故障裕度的影响。

在这个例子中，子系统1、2的组合可允许声明最高硬件安全完整性等级为SIL2（见本示例a)），而子系统4、5的组合可允许声明的最高为SIL1（见本示例b)）。然而，若子系统1、2的组合中出现故障，安全功能能够通过子系统4、5的组合实现。考虑到这种影响，子系统1、2的组合所能达到的硬件故障裕度可增加1级。硬件故障裕度加1可影响所声明的硬件安全完整性等级增加1级（见表2、表3）。因此，关于硬件故障裕度和安全失效分数，子系统1、2、4、5的组合具有可声明的最高硬件安全完整性等级SIL3（也就是子系统1、2的组合所能达到的硬件安全完整性等级（这里为SIL2）加1）。

d) 整个E/E/PE安全相关系统：根据硬件故障裕度，所考虑的安全功能可声明的硬件安全完整性等级要通过分析子系统1、2、4、5（达到SIL3的故障裕度要求，见本示例c））和子系统3（达到SIL2的故障裕度要求）的组合来确定。由于本例中的子系统3达到的硬件安全完整性等级最低，为SIL2，决定了整个E/E/PE安全相关系统的最高硬件安全完整性等级。因此，就这个例子来说，根据硬件故障裕度，安全功能所能达到的最高硬件安全完整性等级是SIL2。



注 1：对于实现安全功能来讲，子系统 1、2 的组合与子系统 4、5 的组合有相同的功能性，并且提供独立的输入到子系统 3。

注 2：子系统实现安全功能要贯穿从传感器到执行器的整个 E/E/PE 安全相关系统。

注 3：充分理解本图，详见 7.4.3.1.6 的例子。

图 6　多通道安全功能的硬件安全完整性的限制示例

7.4.3.2　估算由于随机硬件失效引起安全功能失效的概率的要求

7.4.3.2.1　根据 7.4.3.2.2 和 7.4.3.2.3 估算由于随机硬件失效引起每个安全功能失效的概率，该概率应该等于或者低于安全要求规范（见 7.2.3.2）中规定的目标失效量。

注 1：对于在低要求操作模式中执行的安全功能来说，目标失效量将用在要求时执行的设计功能的平均失效概率表示，如同由安全功能的安全完整性等级所确定的一样（见 GB/T 20438.1—2006 的表 2），除非在 E/E/PES 的

安全完整性要求规范(见 7.2.3.2)中要求安全功能,要满足特定的目标失效量而不是特定的 SIL。例如,为了达到所需的风险降低,当规定目标失效量为 1.5×10^{-6}(在要求时的失效概率)时,那么由于随机硬件失效造成的安全功能在要求时的失效概率要等于或低于 1.5×10^{-6}。

注 2:对于在高要求/连续操作模式中执行的安全功能来说,目标失效量将用每小时危险失效的平均概率来表示,如同由安全功能的安全完整性等级所确定的一样(见 GB/T 20438.1—2006 的表 3),除非在 E/E/PES 的安全完整性要求规范(见 7.2.3.2)中要求安全功能,要满足特定的目标失效量而不是特定的 SIL。例如,为了达到所需的风险降低,当规定目标失效量为 1.5×10^{-6}(每小时危险失效概率)时,那么由随机硬件失效造成的安全功能的失效概率需等于或低于 1.5×10^{-6}(每小时危险失效概率)。

注 3:为了示范已经达到本条的要求,有必要使用一种恰当的技术(见 7.4.3.2.2)对相关安全功能执行可靠性预测,并将结果与相关安全功能的安全完整性要求的目标失效量进行比较(见 GB/T 20438.1—2006 的表 2、表 3)。

7.4.3.2.2 估算由于随机硬件失效造成的每个安全功能的失效概率应考虑的因素:

a) 与所考虑的每个安全功能相关的 E/E/PE 安全相关系统的结构;

注 1:包括决定子系统的哪种失效模式是串联配置(即:任何失效都可造成将执行的相关安全功能的失效)和哪种是并联配置(即:相关安全功能的失效必需是并发失效)。

b) 在任何能造成 E/E/PE 安全相关系统危险失效但能通过诊断测试检测到这种危险失效的模式下,估算出的每个子系统的失效率(见 7.4.7.3 和 7.4.7.4);

c) 在任何能造成 E/E/PE 安全相关系统危险失效但不能通过诊断测试检测到这种危险失效的模式下,估算出的每个子系统的失效率(见 7.4.7.3 和 7.4.7.4);

d) E/E/PE 安全相关系统对共同原因失效的敏感性(见注 2 和注 11);

注 2:例如,见 GB/T 20438.6—2006 的附录 D。

e) 诊断测试的诊断覆盖率(根据附录 C 确定)和相关的诊断测试间隔;

注 3:诊断测试间隔和随后的修理时间共同组成了平均恢复时间,该参数将在可靠性模型中考虑。而且,对于在高要求或连续操作模式下工作的 E/E/PE 安全相关系统,某个通道的任何危险失效都会导致 E/E/PE 安全相关系统的危险失效,如果诊断测试间隔比预期的要求率低不到一个量级(见 7.4.3.2.5),那么在可靠性模型中就需要直接考虑诊断测试间隔(即除考虑平均恢复时间外)。

注 4:在建立诊断测试间隔时,要考虑对诊断覆盖率有贡献的所有测试之间的间隔。

f) 用来揭露未被诊断测试检测到的危险故障而执行检验测试的间隔;

g) 对已检测到的失效的修理时间;

注 5:修理时间是平均恢复时间的一部分(见 IEV 191-13-08),平均恢复时间还包括检测失效所用的时间和不能执行修理的时间(GB/T 20438.6—2006 的附录 B 提供了如何利用平均恢复时间来计算失效概率的一个示例)。对于只能在特定的时间段执行修理的情况,例如 EUC 关闭和处于安全状态,要充分考虑不能执行修理的时间段,特别是这段时间相对较长时。

h) 任何数据通信过程中未检测到的失效的概率(见注 11 和 7.4.8.1)。

注 6:GB/T 20438.6—2006 的附录 B 描述了一种简易的方法,可用来估算由于随机硬件失效引起安全功能危险失效的概率,从而确定结构是否满足所需的目标失效量。

注 7:GB/T 20438.6—2006 附录 A 的 A.2 提供了为达到所需的硬件安全完整性必需的步骤的概述,并显示了该条与 GB/T 20438 其他要求的关联。

注 8:对于每个安全功能,将 E/E/PE 安全相关系统的可靠性分开进行量化是十分必要的,因为使用了不同的部件失效模式,并且 E/E/PE 安全相关系统的结构(根据冗余)也可能改变。

注 9:可以应用的建模方法很多,选择最恰当的方法是分析员的事,要依赖于具体情况,可采用的方法包括:

——因果图分析(见 GB/T 20438.7—2006 附录 B 的 B.6.6.2);

——故障树分析(见 GB/T 20438.7—2006 附录 B 的 B.6.6.5);

——马尔可夫模型(见 GB/T 20438.7—2006 附录 C 的 C.6.4);

——可靠性框图(见 GB/T 20438.7—2006 附录 C 的 C.6.5)。

注 10:在可靠性模型中考虑平均恢复时间(见 IEV 191-13-08)时,要把诊断测试间隔、修理时间和恢复之前的任何其他延误都考虑进去。

注 11：由共同原因诱发的以及数据通信过程中造成的失效与硬件部件的实际失效的起因(例如，电磁干扰、解码错误等)不同。然而根据 GB/T 20438 的目的将这些失效考虑为随机硬件失效。

7.4.3.2.3 任何一个硬件故障裕度大于零的子系统的诊断测试间隔应能使 E/E/PE 安全相关系统满足随机硬件失效概率的要求(见 7.4.3.2.1)。

7.4.3.2.4 任何一个硬件故障裕度等于零、安全功能是完全依赖该子系统(见注 1)且只在低要求模式工作下实现安全功能的子系统，其诊断测试间隔应能使 E/E/PE 安全相关系统满足随机硬件失效概率的要求(见 7.4.3.2.1)。

注 1：如果子系统的失效可造成考虑下的 E/E/PE 安全相关系统内的安全功能的失效，且该安全功能也没有分配给其他安全相关系统时，该安全功能被认为是完全依赖于该子系统的(见 GB/T 20438.1—2006 的 7.6)。

注 2：当子系统输出状态的某种组合有可能直接引起危险事件发生(如危险和风险分析所确定的那样，见 GB/T 20438.1—2006 的 7.4.2.10)，以及当不能确定子系统中输出状态的组合是否在有故障的情况下时(例如 B 类子系统的情况下)，有必要将子系统中的危险故障的检测看作是在高要求或连续模式下工作的安全功能，并且要应用 7.4.6.3 和 7.4.3.2.5 的要求。

7.4.3.2.5 任何一个硬件故障裕度等于零、安全功能是完全依赖该子系统的(见注 1)且在高要求或连续操作模式下工作实现任意安全功能的子系统，其诊断测试间隔应满足：诊断测试间隔与为实现或维持安全状态而执行规定动作(故障反应)(见 7.2.3.1 g))所用时间的总和小于过程安全时间。过程安全时间的定义为：从在 EUC 内或 EUC 控制系统(有导致危险事件发生的隐患)中发生失效到如果不执行安全功能而发生危险事件之间的时间段。

注 1：如果子系统的失效可造成所考虑的 E/E/PE 安全相关系统内的安全功能的失效，且该安全功能也没有分配给其他安全相关系统时，该安全功能被认为是完全依赖于该子系统的(见 GB/T 20438.1—2006 的 7.6)。

注 2：对于执行特殊安全功能的子系统，若诊断测试率与要求率之比大于 100，假设其所提供的安全功能不用于阻止可能导致危险事件发生的输出状态组合(见注 3)，那么该子系统将被视为在低要求操作模式下实现安全功能(见 7.4.3.2.4)。

注 3：如果安全功能用于阻止可能直接导致危险事件发生的特殊输出状态组合，则有必要将该安全功能视为在高要求或连续模式下操作(见 7.4.2.12)。

7.4.3.2.6 对于特殊设计，如果相关安全功能没有达到安全完整性要求的目标失效量，则应：

——确定对安全而言的关键部件、子系统和/或参数；

——评价可能的改进措施对安全而言的关键部件、子系统或参数的影响(例如，更可靠的部件，应付共同模式失效的附加防御，增大诊断覆盖率，增加冗余，降低验证测试间隔，等等)；

——选择和实现适用的改进措施；

——重复必要的步骤以确定一个新的硬件失效概率。

7.4.4 避免失效的要求

注：7.4.4.1～7.4.4.6 不适用于满足“经使用证实”要求的子系统(见 7.4.7.6～7.4.7.12)。

7.4.4.1 应使用一组恰当的技术和措施，用于在 E/E/PE 安全相关系统硬件的设计和开发期内防止引入故障(见表 B.2)。

7.4.4.2 根据所需的安全完整性等级，所选择的设计方法具有的特性应有助于：

a) 透明性、模块化和控制复杂性的其他特性。

b) 清晰和精确地表述：

——功能性；

——子系统接口；

——排序和时间关联信息；

——并发性和同步化。

c) 信息的通信和清晰、准确的文档化。

d) 验证和确认。

7.4.4.3 为保证 E/E/PE 安全相关系统的安全完整性能保持在所需的等级，在设计阶段就应将维护要求规范化。

7.4.4.4 如适用，应使用自动测试工具和集成开发工具。

7.4.4.5 设计期间，应编制 E/E/PES 的集成测试计划。编制测试计划的文档应包括：

a) 所执行测试的类型和所遵循的规程；

b) 测试环境、工具、配置和程序；

c) 测试是否通过的准则。

7.4.4.6 设计期间，根据开发者提出的前提条件可执行的那些活动，应该与在用户立场上所要求的活动加以区分。

7.4.5 控制系统故障的要求

注：7.4.5.1～7.4.5.3 不适用于满足“经使用证实”要求的子系统（见 7.4.7.6～7.4.7.12）。

7.4.5.1 为控制系统故障，E/E/PES 的设计特点应使得 E/E/PE 安全相关系统能容许：

a) 如果不能排除硬件设计故障的可能性（见表 A.16），硬件中的任何残余设计故障；

b) 环境应力，包括电磁干扰（见表 A.17）；

c) EUC 操作员造成的失误（见表 A.18）；

d) 软件中的任何残余设计故障（见 GB/T 20438.3—2006 的 7.4.3 及相关的表）；

e) 任何数据通信过程中产生的错误和其他影响（见 7.4.8）。

7.4.5.2 在设计和开发活动中应考虑可维护性和可测试性，以便在最终的 E/E/PE 安全相关系统中实现这些属性。

7.4.5.3 E/E/PE 安全相关系统的设计应充分考虑人员的能力和局限性，并应适合分配给操作者和维护人员的行动。所有接口的设计应根据良好的人员操作习惯并应适合操作者的认知能力和培训水平，例如对于批量生产中的 E/E/PE 安全相关系统，操作者只是公众的一员。

注 1：设计目标应该是，对操作者和维护人员所犯的可预见的致命失误，只要有可能都应能通过设计来防止和消除，或者在完成该动作之前对这些动作进行二次确认。

注 2：一些由操作人员或维护人员造成的失误也许不能被 E/E/PE 安全相关系统修复，例如，除通过直接检查外是不能检测到的或不能被实际修复的，如在 EUC 内部的一些机械失效。

7.4.6 故障检测时对系统行为的要求

7.4.6.1 在硬件故障裕度大于零的子系统中，对检测出的危险故障（通过诊断测试，检验测试或其他方法）应采取：

a) 某个规定动作以达到或维持安全状态（见注）；或者

b) 隔离子系统的故障部分，以允许 EUC 继续安全工作，同时修理故障部分。如果在计算随机硬件失效概率（见 7.4.3.2.2）时设定的平均恢复时间（MTTR）内未完成修理，那么应该采取某一规定的动作以达到或维持安全状态（见注）。

注：在 E/E/PES 安全要求（见 7.2.3.1）中规定为达到或维持安全状态需采取的规定动作（故障反应）。可能采取的动作包括，例如，安全关闭 EUC，或者为降低风险，安全关闭与故障子系统相关的 EUC 部分。

7.4.6.2 对于硬件故障裕度等于零以及安全功能完全依赖该子系统（见注 1）的子系统，当该子系统仅在低要求模式下运行安全功能时，对检测出的危险故障（通过诊断测试，检验测试或其他方法）应采取：

a) 某个规定动作以达到或维持安全状态，或者

b) 在计算随机硬件失效概率（见 7.4.3.2.2）时设定的平均恢复时间（MTTR）内，修理故障子系统。在此期间内，EUC 的连续安全应通过附加措施和约束来保证。这些措施和约束提供的风险降低至少应等于无任何故障的 E/E/PES 安全相关系统提供的风险降低。应在 E/E/PES 操作和维护规程中对附加措施和约束进行规定（见 7.6）。如果在规定的平均恢复时间（MTTR）内，不能进行修理，那么应该采取其他规定的动作以达到或维持安全状态（见注 2）。

注 1：如果子系统的失效可造成所考虑的 E/E/PE 安全相关系统内的安全功能的失效，且该安全功能也没有分配给

其他安全相关系统时，该安全功能被认为是完全依赖于该子系统的(见 GB/T 20438.1—2006 的 7.6)。

注 2：在 E/E/PES 安全要求(见 7.2.3.1)中规定为达到或维持安全状态需采取的规定动作(故障反应)。可能采取的动作包括，例如，安全关闭 EUC，或者为降低风险，安全关闭与故障子系统相关的 EUC 部分。

7.4.6.3 对于硬件故障裕度大于零以及安全功能完全依赖该子系统(见注 1)的子系统，当该子系统在高要求或连续操作模式(见注 2、注 3)下运行安全功能时危险故障的检测(通过诊断测试，检验测试或其他方法)将导致规定的动作以达到或维持安全状态(见注 3)。

注 1：如果子系统的失效可造成所考虑的 E/E/PE 安全相关系统内的安全功能的失效，且该安全功能也没有分配给其他安全相关系统时，该安全功能被认为是完全依赖于子系统的(见 GB/T 20438.1—2006 的 7.6)。

注 2：当子系统输出状态的某种组合有可能直接引起危险事件发生(如同危险和风险分析所确定的那样，见 GB/T 20438.1—2006 的 7.4.2.10)，以及当不能确定子系统在有故障的情况下输出状态的组合时(例如在 B 类子系统的情况下)，有必要将子系统中的危险故障的检测看作是在高要求或连续模式下工作的安全功能，并且应当应用 7.4.6.3 和 7.4.3.2.5 的要求。

注 3：在 E/E/PES 安全要求(见 7.2.3.1)中规定为达到或维持安全状态需采取的规定动作(故障反应)。可能采取的动作包括，例如，安全关闭 EUC，或者为降低风险，安全关闭与故障子系统相关的 EUC 部分。

7.4.7 E/E/PES 实现的要求

7.4.7.1 根据 E/E/PES 的设计来实现 E/E/PES 安全相关系统。

7.4.7.2 被一个或多个安全功能使用的所有子系统都应作为安全相关子系统进行标识和文档化。

7.4.7.3 对于每一个安全相关子系统(见 7.4.7.4)应提供下列信息：

a) 功能的功能性规范和安全功能使用的子系统的接口；

b) 在危险失效可由诊断测试检测出的情况下，在任何模式下能引起 E/E/PE 安全相关系统危险失效的估算失效率(由随机硬件失效引起)(见 7.4.7.4)；

c) 在危险失效用诊断测试检测不到的情况下，在任何模式下能引起 E/E/PE 安全相关系统危险失效的估算失效率(由随机硬件失效引起)(见 7.4.7.4)；

d) 为保持由于随机硬件失效引起的估算失效率的有效性，子系统应遵照的环境限制；

e) 为保持由于随机硬件失效引起的估算失效率的有效性，子系统不得超过的寿命限制；

f) 定期检验测试和/或维护要求；

g) 根据附录 C 得出的诊断覆盖率(需要时见注 1)；

h) 诊断测试间隔(需要时见注 1)；

注 1：上述 g)和 h)与子系统内部的诊断测试有关。本信息仅当在 E/E/PE 安全相关系统可靠性模型中为子系统内执行的诊断测试行动声明置信度时才需要(见 7.4.3.2.2)。

i) 诊断发现故障后为能推导出平均恢复时间(MTTR)所必需的附加信息(例如修理时间)；

注 2：为了能估算出在要求时的失效概率，或每小时安全功能的失效概率(见 7.4.3.2.2)，需要上述 b)～ i)项的内容。

注 3：b)，c)，g)，h)和 i)项仅作为某些子系统的独立参数才需要，这些子系统如传感器和执行器可被组合成冗余结构，以提高硬件安全完整性，而对于某些子系统如逻辑解算器，它们本身在 E/E/PE 安全相关系统内并不组合成冗余结构，根据要求时的失效概率或每小时的危险失效概率，考虑 b)，c)，g)，h)和 i)项来规定性能是可以接受的。对这些项来说，有必要建立未检测到的失效的检验测试间隔。

j) 根据附录 C 确定的、能推导出子系统用于 E/E/PE 安全相关系统中时的安全失效分数(SFF)的所有信息；

k) 子系统的硬件故障裕度；

注 4：根据结构约束(见 7.4.3.1)来确定安全功能所能声明的最高安全完整性等级时需要 j)和 k)项。

l) 为避免系统失效，应遵循的对子系统应用的任何限制；

m) 某个安全功能所能声明的最高安全完整性等级，该安全功能使用子系统时，应基于：

——在子系统硬件和软件的设计和实现过程中为防止引入系统故障所使用的技术和措施(见 7.4.4.1 和 GB/T 20438.3—2006 的 7.4)。

——使子系统能容许系统故障的设计特性(见 7.4.5.1);

注 5:对于那些经使用证实的子系统不作要求(见 7.4.7.5)。

n) 为了使 E/E/PE 安全相关系统的配置管理符合 GB/T 20438.1—2006 中 6.2.1 的要求,需要识别子系统硬件和软件配置的所有信息;

o) 证明子系统经过确认的文档化证据。

7.4.7.4 由于随机硬件失效造成的子系统的失效的估算失效率(见 7.4.7.3 b)和 c))可:

a) 利用公认的、来源于工业的部件失效数据,通过设计失效模式和效应分析来确定;

注 1:所使用的任何失效率数据至少应达到 70%的置信度水平。置信度水平的统计确定在 IEEE 352 中被定义。IEC 61164 中使用另外一个等价术语——有效性水平。

注 2:最好能获得具体现场的失效数据,否则,可采用通用数据。

注 3:大多数概率估算方法假定失效率为一恒量,但前提条件是部件没有超过使用寿命。超过使用寿命(即当失效的概率随时间推移大幅度地增长)大多数概率计算方法的结果也就失去了意义。因此,任何概率估算要包括部件使用寿命的规范。使用寿命高度依赖于部件本身和工作条件——特别是温度(例如,电解质容器可能是非常敏感的)。经验表明,使用寿命往往在 8~12 年之间。然而,总是在接近规范极限下工作的部件,其寿命将可能大大降低。部件的使用寿命越长往往造价越高。

b) 或基于以往在类似环境条件下使用子系统的经验来确定(见 7.4.7.9)。

7.4.7.5 对于认为是经使用证实的子系统(见 7.4.7.6),不要求提供用于预防和控制系统故障的技术和措施的有关信息(见 7.4.7.3 m))。

7.4.7.6 对于以往开发的子系统,只有在功能性规定明确、有充分文档依据表明子系统的具体配置此前确实应用过(使用时的所有失效记录均登记在册,见 7.4.7.10)、以及考虑过任何所需的附加分析和测试(见 7.4.7.8)时,才能被认为是经使用证实的子系统。文档依据应显示 E/E/PE 安全相关系统子系统的任何失效(由随机硬件和系统故障造成)的可能性足够低,可以达到使用子系统的安全功能所需的安全完整性等级。

7.4.7.7 为了确定任何未被检测到的系统故障的可能性足够低,可以达到使用子系统的安全功能所需的安全完整性等级,7.4.7.6 要求的文档应显示出具体子系统以往的使用条件(见注)与在 E/E/PE 安全相关系统中子系统将要经历的条件相同或者非常接近。

注:使用条件(操作行规)包括可能影响子系统硬件和软件内系统故障可能性的所有因素。例如,环境、使用模式、执行的功能、配置、与其他系统的接口、操作系统、翻译器、人为因素。

7.4.7.8 如果以往的使用条件与在 E/E/PE 安全相关系统内将要经历的条件存在差异,应当对这些差异加以标识,并结合恰当的分析方法和测试对这些差异进行明确地例示,以便确定任何未被揭露出的系统故障的可能性足够低,以致可以达到使用子系统的安全功能所需的安全完整性等级。

7.4.7.9 7.4.7.6 要求的文档证据应确定以往子系统的专用配置的使用程度(用工作小时表示)在统计学基础上足以支持所声明的失效率。最低限度,需要足够的工作时间才能确立所声明的失效率数据的置信度单边下限值至少能达到 70%(见 GB/T 20438.7—2006 附录 D 和 IEEE 352),任何工作时间不超过一年的单个子系统在统计分析中不作为计算总工作时间的一部分(见注)。

注:确立所声明的失效率所必需的工作小时可以用许多相同子系统的工作时间来确定,但条件是所有这些子系统的失效都已被有效检测并已报告(见 7.4.7.10)。例如,如果 100 个子系统每个无故障工作 10 000 h,那么总无故障工作时间就可认为是 1 000 000 h。在此,每个子系统的使用时间均超过一年,因此总工作时间要把所有子系统的工作时间都算在内。

7.4.7.10 在确定是否满足上述要求(7.4.7.6~7.4.7.9)时,仅考虑以前的将子系统的全部失效有效地检测和报告的操作(例如,当按照 IEC 60300-3-2 推荐已收集了失效数据时)。

7.4.7.11 在根据可用信息的广度和深度(见 GB/T 20438.1—2006 的 4.1),确定是否满足上述要求(7.4.7.6~7.4.7.9)时,应考虑以下因素:

a) 子系统的复杂性;

b) 子系统对降低风险所起的作用；

c) 子系统失效产生的后果；

d) 设计的新颖性。

7.4.7.12 在E/E/PE安全相关系统中，对“经使用证实”的安全相关子系统的应用只局限于在满足相关要求(见7.4.7.6～7.4.7.10)的子系统的那些功能和接口。

注：7.4.7.4～7.4.7.12中的措施也适用于包含软件的子系统。在这种情况下，要保证在安全应用中子系统只执行安全完整性证据已给出的那个功能，见GB/T 20438.3—2006的7.4.2.11。

7.4.8 数据通信的要求

7.4.8.1 当在安全功能的实现中使用任何数据通信格式时，那么在估算通信过程中未检测到的失效概率时，应将传输差错、重复、删除、插入、重新排序、误用、延时和伪装等因素考虑进去(见7.4.8.2)。在估算由随机硬件失效(见7.4.3.2.2)引起安全功能危险失效的概率时应考虑此概率。

注：伪装一词的意思是报文的真实内容没有被正确地鉴别。例如，来自非安全部件的报文错误地被鉴别为来自安全部件的报文。

7.4.8.2 特别是在估算由通信过程引起安全功能失效的概率时，应考虑如下参数：

a) 残余错误率(见IEV 371-08-05)；

b) 残余信息丢失率(见IEV 371-08-09)；

c) 信息传送率(比特率)的限制和可变性；

d) 信息传播延时的限制和可变性。

注1：每小时危险失效率等于残余错误率除以报文长度(二进制数位)，乘以与安全有关的报文的总线传输率，再乘以系数3 600。

注2：进一步信息可见IEC 60870-5-1、EN 50159-1和EN 50159-2。

7.5 E/E/PES集成

注：这一阶段是图2的方框9.4。

7.5.1 目的

集成和测试E/E/PE安全相关系统。

7.5.2 要求

7.5.2.1 E/E/PE安全相关系统应按照规定的E/E/PES设计进行集成，并按照规定的E/E/PES集成测试(见7.4.2.11)进行测试。

7.5.2.2 所有模块集成到E/E/PE安全相关系统后，E/E/PE安全相关系统应该按照要求(见7.4)进行测试。这些测试应显示所有模块能够正确地相互作用并执行预期功能，而不执行非预期的功能。

注1：这并不意味着对所有输入组合进行测试。对所有等价类进行测试(见GB/T 20438.7—2006的B.5.2)可能就足够了。静态分析(见GB/T 20438.7—2006的B.6.4)、动态分析(见GB/T 20438.7—2006的B.6.5)或者失效分析(参见GB/T 20438.7—2006的B.6.6)可以减少测试用例的数量到一个可接受的程度。如果按照结构化设计(见GB/T 20438.7—2006的B.3.2)或者半形式化方法(见GB/T 20438.7—2006的B.2.3)规则来进行开发，与不用这些方法相比能够更容易满足要求。

注2：在使用形式化方法(见GB/T 20438.7—2006的B.2.2)、形式化检验或断言(见GB/T 20438.7—2006的C.5.13和C.3.3)进行开发时，可减少测试范围。

注3：同样也可使用统计证据(见GB/T 20438.7—2006的B.5.3)。

7.5.2.3 PES中安全软件的集成应按照GB/T 20438.3—2006的7.5执行。

7.5.2.4 应产生适当的E/E/PE安全相关系统的集成测试文档，声明测试结果，同时声明在设计与开发阶段的目标和准则是否得到满足。如果存在失效，应将失效原因和纠正方法文档化。

7.5.2.5 在集成和测试期间，对于E/E/PE安全相关系统的任何修正或改变，应进行影响分析从而识别所有受影响的部件并进行必要的重新验证活动。

7.5.2.6 E/E/PES集成测试应文档化以下信息：

a) 使用的测试规范的版本；

b) 可接受的集成测试准则；

c) 被测试 E/E/PE 安全相关系统的版本；

d) 校准数据及所使用的工具和设备；

e) 每次测试的结果；

f) 预期值和实际结果之间的任何差异；

g) 当发现差异时，对是否继续测试或发布修改请求而做出的分析和决策。

7.5.2.7 为避免在 E/E/PES 集成期间出现故障，应根据表 B.3 采用一组恰当的技术和措施。

7.6 E/E/PES 操作和维护规程

注：这一阶段是图 2 的方框 9.5。

7.6.1 目的

制定规程以确保在操作和维护期间保持 E/E/PE 安全相关系统所要求的功能安全。

7.6.2 要求

7.6.2.1 制定 E/E/PES 的操作和维护规程应规定如下内容：

a) 为保持“符合设计的”E/E/PE 安全相关系统的功能安全需执行的日常活动，包括预定义寿命部件的日常替换，如冷却风扇、电池，等等。

b) 为防范不安全状态和/或降低危险事件造成的后果所必需的活动和约束（例如，在安装、启动、正常操作、日常测试、可预见的干扰、故障或失效，以及停机期间）。

c) 需保持的有关 E/E/PE 安全相关系统的失效和要求率的文档。

d) 需要保持的能显示 E/E/PE 安全相关系统的审核和测试结果的文档。

e) 当在 E/E/PE 安全相关系统出现故障或失效时，应遵循的维护规程，包括：

——故障诊断和修理的规程；

——重新确认的规程；

——维护报告要求。

f) 应规定的用于报告维护执行的规程，特别是：

——报告失效的规程；

——分析失效的规程。

g) 维护和重新确认所必需的工具以及工具和设备维护的规程。

注 1：出于安全和经济的考虑，把 E/E/PES 的操作和维护规程与 EUC 整体的操作和维护规程集成在一起是有益的。

注 2：E/E/PES 的操作和维护规程应包括软件修改规程（见 GB/T 20438.3—2006 的 7.8）。

7.6.2.2 E/E/PE 安全相关系统的操作和维护规程应根据输入，比如：a）功能安全审核的结果；b）E/E/PE 安全相关系统测试的结果，不断升级。

7.6.2.3 为保持 E/E/PE 安全相关系统要求的功能安全（符合设计的）所需的日常维护行动应由系统方法确定。这种方法可确定所有安全部件（从传感器到最终元件）的未揭露出的失效，这些失效将导致安全完整性等级的降低。适用的方法包括：

——故障树测验；

——失效模式和效应分析；

——可靠性集中维护。

注 1：在确定要求的行动和恰当的 E/E/PE 安全相关系统接口时，人为因素是要考虑的关键因素。

注 2：检验测试的执行应以一定的频率进行，以达到目标失效量的要求。

注 3：检验测试的频率，诊断测试间隔和随后修理所需的时间将依赖于以下几个因素（见 GB/T 20438.6—2006 的附录 B）：

——与安全完整性等级相关的目标失效量；

——结构；

——诊断测试的诊断覆盖率，以及

——预期的要求率。

注4：检验测试频率和诊断测试间隔对达到硬件安全完整性有决定性的意义。执行硬件可靠性分析(见7.4.3.2.2)的一个主要原因是保证两类测试的频率适合于目标硬件安全完整性。

7.6.2.4 应评估E/E/PES操作和维护规程可能会对EUC造成的影响。

7.6.2.5 为在E/E/PES操作和维护规程中避免出现故障和失效，应根据表B.4采用一组恰当的技术和措施。

7.7 E/E/PES的安全确认

注：这一阶段是图2的方框9.6。

7.7.1 目的

根据要求的安全功能和安全完整性确认E/E/PE安全相关系统在所有方面都能满足安全要求(见7.2)。

7.7.2 要求

7.7.2.1 E/E/PES安全确认应按照预定计划执行(另见GB/T 20438.3—2006的7.7)。

注1：在E/E/PES安全生命周期中显示，E/E/PES安全确认是在安装之前执行的，但在某些情况下，E/E/PES安全确认直到安装之后才能执行(例如，应用软件的开发工作直到安装之后才完成)。

注2：可编程电子安全相关系统的确认包括硬件和软件的确认。软件的确认要求在GB/T 20438.3中说明。

7.7.2.2 所有用于确认的测量设备应依据有据可查的国家标准，或者如果可能，依据公认的规程进行校准。所有测试设备应进行操作正确性验证。

7.7.2.3 在E/E/PES安全要求(见7.2)中规定的每一个安全功能，以及所有E/E/PES操作和维护规程都应通过测试和/或分析来确认。

7.7.2.4 应为所有安全功能制定适用的E/E/PE安全确认测试的说明文档，说明的内容包括：

a) E/E/PES安全确认计划使用的版本；

b) 被测试(或分析)的安全功能，以及专门引用的在编制E/E/PES安全确认计划过程中所规定的要求；

c) 校准数据及所使用的工具和设备；

d) 每次测试的结果；

e) 预期值和实际结果之间的任何差异。

注：不需要为每一个安全功能建立独立的文档，但是a)～e)各项中的信息要应用于所有安全功能，在安全功能不同时要说明其关系。

7.7.2.5 当出现差异(即实际的结果偏离预期结果的幅度大于所声明的裕度)时，应将E/E/PES安全确认测试的结果记录在文档中，包括：

a) 所做的分析；以及

b) 所做的决策：继续测试或发布修改请求并返回确认测试的较早部分。

7.7.2.6 供应商或开发者应为EUC和EUC控制系统开发者提供E/E/PES安全确认测试结果，以使它们能满足GB/T 20438.1中的整体安全确认要求。

7.7.2.7 为在E/E/PES安全确认中避免出现故障，应根据表B.5采用一组恰当的技术和措施。

7.8 E/E/PES的修改

7.8.1 目的

保证在对E/E/PE安全相关系统进行改正、加固和适应之后保持要求的安全完整性不变。

7.8.2 要求

7.8.2.1 应当为每次E/E/PES的修改活动建立和保持适用的文档记录，文档应包括：

a) 修改或变更的详细规范；

b) 修改活动对整个系统包括硬件、软件(见 GB/T 20438.3)、人员因素、环境和可能的相互作用的影响分析;

c) 所有变更的批准;

d) 变更所带来的改进;

e) 部件的测试用例,包括重新确认数据;

f) E/E/PES 配置管理的历史;

g) 与正常操作和条件的偏差;

h) 系统规程的必要变更;

i) 文档的必要变更。

7.8.2.2 声明全部或部分符合 GB/T 20438 的制造商和系统供应商应维护系统,以便在检测到软件和硬件的缺陷时着手进行更改,并把在影响安全的缺陷事件中进行修改的必要性通知用户。

7.8.2.3 应该在至少与 E/E/PE 安全相关系统初始开发相同的专业水平、自动化工具(见 GB/T 20438.3—2006 的 7.4.4.2)、计划编制和管理程度下执行修改。

7.8.2.4 修改之后,E/E/PE 安全相关系统应重新验证和重新确认。

注:另见 GB/T 20438.1—2006 的 7.16.2.6。

7.9 E/E/PES 的验证

7.9.1 目的

测试和评估给定阶段的输出,以保证作为该阶段所提供的输入的产品和标准的正确性和一致性。

注:为了方便起见,所有验证活动都在 7.9 中规定,而实际上它们的执行跨越了几个阶段。

7.9.2 要求

7.9.2.1 对于 E/E/PES 安全生命周期的每一阶段,E/E/PE 安全相关系统的验证应与开发(见 7.4)同时拟制计划并建立文档。

7.9.2.2 编制 E/E/PES 验证计划时应参照在该阶段验证中有关的所有的准则、技术和工具。

7.9.2.3 编制 E/E/PES 验证计划时应规定要执行的具体活动,以保证作为阶段所提供的输入的产品和标准的正确性和一致性。

7.9.2.4 编制 E/E/PES 验证计划时应考虑以下内容:

a) 验证策略和技术的选择;

b) 测试设备的选择和利用;

c) 验证活动的选择和文档;

d) 对直接从验证设备和测试中获取的验证结果的评价。

7.9.2.5 在每个设计和开发阶段中,应能显示出已达到功能和安全完整性的要求。

7.9.2.6 每个验证活动的结果都应文档化,内容包括:E/E/PE 安全相关系统已通过验证或失效原因的说明。应考虑以下因素:

a) 与一个或多个 E/E/PES 安全生命周期相关要求不相符的条款(见 7.2);

b) 与一个或多个相关设计标准不相符的条款(见 7.4);

c) 与一个或多个相关安全管理要求不相符的条款(见第 6 章)。

7.9.2.7 对于 E/E/PES 安全要求验证,在建立 E/E/PES 安全要求(见 7.2)之后和在下一阶段(设计和开发)开始之前,验证应:

a) 针对在安全计划期间所规定的安全性、功能性和其他要求,确定 E/E/PES 安全要求是否充分满足在 E/E/PES 安全要求分配(见 GB/T 20438.1)中提出的要求;以及

b) 检查以下各项间的不兼容性:

——E/E/PES 安全要求(见 7.2);

——安全要求分配(GB/T 20438.1);

——E/E/PES 测试(见 7.4);以及

——用户文档和所有其他系统文档。

7.9.2.8 对于 E/E/PES 设计和开发验证,在完成 E/E/PES 设计和开发(见 7.4)之后和在下一阶段(集成)开始之前,验证应:

a) 确定 E/E/PES 测试(见 7.4)是否适用于 E/E/PES 设计和开发(见 7.4)。

b) 确定 E/E/PES 设计和开发(见 7.4)在 E/E/PES 安全要求(见 7.2)方面的一致性和完整性(下至模块级)。

c) 检查下列各项间的不兼容性:

——E/E/PES 安全要求(见 7.2);

——E/E/PES 设计和开发(见 7.4);以及

——E/E/PES 测试(见 7.4)。

注 1:表 B.5 推荐的安全确认、失效分析和测试技术,同样也可适用于验证。

注 2:在验证已达到要求的诊断覆盖率时,可考虑表 A.1 中提供的必须检测的故障和失效。

7.9.2.9 E/E/PES 集成验证,是对 E/E/PE 安全相关系统的集成进行验证,以确定已经达到 7.5 的要求。

7.9.2.10 测试用例和结果应文档化。

8 功能安全评估

功能安全评估的要求在 GB/T 20438.1—2006 的第 8 章中做了详细说明。

附 录 A
（规范性附录）
用于 E/E/PE 安全相关系统的技术和措施：操作中的失效控制

A.1 一般要求

本附录应与 7.4 一起使用。它限制了所声明的有关技术和措施的最大诊断覆盖率。对每一安全完整性等级，本附录对用于控制随机硬件、系统、环境和操作失效的技术和措施提出了建议。有关结构和措施的更多信息可参见 GB/T 20438.6—2006 的附录 B 和 GB/T 20438.7—2006 的附录 A。

无法列出导致复杂硬件失效的所有独立的物理原因，两个主要原因是：

——故障和失效之间的原因或影响关系通常难以确定；

——当使用复杂硬件和软件时，失效的重点将从随机失效转变为系统失效。

E/E/PE 安全相关系统的失效可以根据起始时间分类为：

——起始于系统安装之前或系统安装之中由故障诱发的失效（例如，软件故障，包括规范和程序故障；硬件故障，包括制造故障和部件选择不当）；

——起始于系统安装之后的由故障或人为失误诱发的失效（例如，硬件随机失效，或不正确使用引起的失效）。

为避免和控制失效，通常需要大量的措施，附录 A 和附录 B 中要求的结构，来自于把措施分成在 E/E/PE 安全生命周期不同阶段用来避免失效的那些措施（附录 B），以及在操作过程中用来控制失效的那些措施（附录 A），控制失效的措施是 E/E/PE 安全相关系统的内在特性。

诊断覆盖率和安全失效分数根据表 A.1 和附录 C 中详述的规程确定。表 A.2～表 A.15 支持表 A.1 的要求，为诊断测试推荐了技术和措施，并推荐了在使用这些技术和措施时可实现的最高等级的诊断覆盖率。这些表并不取代附录 C 的任何要求。表 A.2～表 A.15 并不详尽，当然还可使用其他技术和措施，只要能提供相应的证据，保证支持所声明的诊断覆盖率。一旦声明了高诊断覆盖率，那么，最低限度至少应用一项每个表中的高诊断覆盖率技术。

同样，表 A.16～表 A.18 为每一安全完整性等级推荐了控制系统失效的技术和措施。表 A.16 为控制系统失效推荐了整体措施（见 GB/T 20438.3）。表 A.17 为控制环境失效推荐了措施，表 A.18 为控制操作失效推荐了措施。大部分控制措施均可根据表 A.19 进行分级。

GB/T 20438.7—2006 的附录 A 给出了这些表中所有技术和措施的描述。GB/T 20438.3 给出了每一安全完整性等级所需的软件技术和措施。GB/T 20438.6—2006 的附录 B 给出了确定 E/E/PE 安全相关系统结构的指南。

遵从本附录中的指南不能保证所要求的安全完整性。考虑下列两点是很重要的：

——所选技术和措施的一致性，及其互补性如何；以及

——哪些技术和措施最适合在设计和开发每个特殊的 E/E/PE 安全相关系统中所遇到的具体问题。

A.2 硬件安全完整性

为达到诊断覆盖率的相应级别（见附录 C），表 A.1 给出了为控制硬件失效而由技术和措施检测出的故障和失效的要求。表 A.2～表 A.15 支持表 A.1 的要求，为诊断测试推荐了技术和措施，并推荐了使用这些技术和措施可实现的最高的诊断覆盖率等级。这些测试可以连续地或定期地进行。这些表并不取代 7.4 的任何要求。表 A.2～表 A.15 并不详尽，当然还可使用其他技术和措施，只要提供相应的证据，保证支持所声明的诊断覆盖率。

注 1：GB/T 20438.7—2006 的附录 A 给出了这些表中所有技术和措施的概述。表 A.2～表 A.15 的第二列给出了要求所在的条款。

注 2：诊断覆盖率的低、中和高 3 级分别定量为 60%、90%和 99%。

表 A.1 在操作过程中要检测的或在推导安全失效分数中要分析的故障或失效

部 件	见 表	对所声明的诊断覆盖率或安全失效分数的要求		
		低(60%)	中(90%)	高(99%)
机电装置	表 A.2	未加电或断电 触点被熔接	未加电或断电 单个触点被熔接	未加电或断电 各触点被熔接 不可靠的导向触点(对于继电器，若按照 EN 50205 或等同标准进行构建和测试，则不假定这种失效) 不可靠的开启(对于定位开关，若按照 EN 60947-5-1 或等同标准构建和测试，则不假定这种失效)
分离硬件	表 A.3，表 A.7，表 A.9，表 A.11			
数字 I/O		固定故障(Stuck-at)	DC 故障模型	DC 故障模型 漂移和振动
模拟 I/O		固定故障(Stuck-at)	DC 故障模型 漂移和振动	DC 故障模型 漂移和振动
电源		固定故障(Stuck-at)	DC 故障模型 漂移和振动	DC 故障模型 漂移和振动
总线	表 A.3			
一般要求	表 A.7	地址固定故障	超时	超时
内存管理单元	表 A.8	(Stuck-at)	错误的地址解码	错误的地址解码
直接内存访问		数据或地址固定故障 (Stuck-at) 无或连续访问	数据和地址的 DC 故障模型 访问时间错误	影响内存数据的所有故障 数据或地址错误 访问时间错误
总线仲裁 (见注 1)		仲裁信号固定故障 (Stuck-at)	无或连续仲裁	无或连续或错误仲裁
CPU	表 A.4、表 A.10			
寄存器，内部 RAM		数据和地址固定故障 (Stuck-at)	数据和地址的 DC 故障模型	数据和地址的 DC 故障模型 内存单元的动态交叉 无寻址、错误寻址或多重寻址
编码和执行，包括标记寄存器		错误编码或不执行	错误编码或错误执行	未定义失效假设
地址计算		固定故障(Stuck-at)	DC 故障模型	未定义失效假设
程序计数器，堆栈指针		固定故障(Stuck-at)	DC 故障模型	DC 故障模型

表 A.1(续)

部　　件	见　　表	对所声明的诊断覆盖率或安全失效分数的要求		
		低(60%)	中(90%)	高(99%)
中断处理	表 A.4	无或连续中断	无或连续中断 中断的交叉	无或连续中断 中断的交叉
不可变内存	表 A.5	数据和地址固定故障(Stuck-at)	数据和地址的 DC 故障模型	影响内存数据的所有故障
可变内存	表 A.6	数据和地址固定故障(Stuck-at)	数据和地址的 DC 故障模型 对于集成度不低于 1Mbits 的 DRAM,软错误引起的信息改变	数据和地址的 DC 故障模型 内存单元的动态交叉 无寻址、错误寻址或多重寻址 对于集成度不低于 1Mbits 的 DRAM,软错误引起的信息改变
时钟(石英)	表 A.12	分谐波或超谐波	分谐波或超谐波	分谐波或超谐波
通信和大容量存储器	表 A.13	错误的数据或地址 不传输	影响内存数据的所有故障 错误的数据或地址 错误的传输时间 错误的传输顺序	影响内存数据的所有故障 错误的数据或地址 错误的传输时间 错误的传输顺序
传感器	表 A.14	固定故障(Stuck-at)	DC 故障模型 漂移和振动	DC 故障模型 漂移和振动
最终元件	表 A.15	固定故障(Stuck-at)	DC 故障模型 漂移和振动	DC 故障模型 漂移和振动

注 1:总线仲裁是一种决定哪个设备具有总线控制权的机制。

注 2:固定故障(Stuck-at)是一种故障种类,可以用部件引脚的连续“0”或“1”或“on”来表示。

注 3:“DC 故障模型”(DC 为直流)包括的失效模式有:固定故障(Stuck-at)、固定开故障(Stuck-open),开路或高阻抗输出以及信号线间的短路。

表 A.2　电 气 子 系 统

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
利用在线监视检测失效	A.1.1	低(低要求模式) 中(高要求或连续模式)	依赖于失效检测的诊断覆盖率
继电器触点监视	A.1.2	高	
比较器	A.1.3	高	若在安全导则中失效模式起支配作用,则高
多数表决器	A.1.4	高	依赖于表决质量
无功电流原理	A.1.5	低	仅对无需用连续控制来实现或维护 EUC 安全状态的 E/E/PE 安全相关系统有效

注 1:本表不取代附录 C 的任何要求。

注 2:附录 C 的要求与诊断覆盖率的确定有关。

注 3:有关本表的一般注释,见表 A.1 前的正文。

表 A.3 电 子 子 系 统

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
利用在线监视检测失效	A.1.1	低(低要求模式) 中(高要求或连续模式)	依赖于失效检测的诊断覆盖率
比较器	A.1.3	高	若在安全导则中失效模式起支配作用,则高
多数表决器	A.1.4	高	依赖于表决质量
利用冗余硬件进行测试	A.2.1	中	依赖于失效检测的诊断覆盖率
动态原则	A.2.2	中	依赖于失效检测的诊断覆盖率
访问端口和边界扫描结构的标准测试	A.2.3	高	依赖于失效检测的诊断覆盖率
监视冗余	A.2.5	高	依赖于冗余和监视程度
带自动检验的硬件	A.2.6	高	依赖于测试的诊断覆盖率
模拟信号监视	A.2.7	低	
注 1:本表不取代附录 C 的任何要求。 注 2:附录 C 的要求与诊断覆盖率的确定有关。 注 3:有关本表的一般注释,见表 A.1 前的正文。			

表 A.4 处 理 单 元

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
比较器	A.1.3	高	依赖于比较的质量
多数表决器	A.1.4	高	依赖于表决的质量
利用软件进行自测试:有限模式数(单通道)	A.3.1	低	
利用软件进行自测试:漫步位(单通道)	A.3.2	中	
由硬件支持的自测试(单通道)	A.3.3	中	
编码处理(单通道)	A.3.4	高	
利用软件进行相互比较	A.3.5	高	依赖于比较的质量
注 1:本表不取代附录 C 的任何要求。 注 2:附录 C 的要求与诊断覆盖率的确定有关。 注 3:有关本表的一般注释,见表 A.1 前的正文。			

表 A.5 不可变内存范围

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
字保存多位冗余	A.4.1	中	
修正的校验和	A.4.2	低	
单字(8bit)的签名	A.4.3	中	签名的有效性依赖于与受保护的信息块长度有关的签名的宽度
双字(16bit)的签名	A.4.4	高	签名的有效性依赖于与受保护的信息块长度有关的签名的宽度
块复制	A.4.5	高	

注 1：本表不取代附录 C 的任何要求。
注 2：附录 C 的要求与诊断覆盖率的确定有关。
注 3：有关本表的一般注释，见表 A.1 前的正文。

表 A.6 可变内存范围

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
“检测板”或“跨步”RAM 测试法	A.5.1	低	
“漫步路径”RAM 测试法	A.5.2	中	
“galpat”或“透明 galpat”RAM 测试法	A.5.3	高	
“Abraham”RAM 测试法	A.5.4	高	
RAM 的奇偶位	A.5.5	低	
利用修改的海明码的 RAM 监视，或利用差错检测和纠错码(EDC)校验数据失效	A.5.6	高	
带硬件或软件比较和读/写测试的双 RAM	A.5.7	高	

注 1：本表不取代附录 C 的任何要求。
注 2：附录 C 的要求与诊断覆盖率的确定有关。
注 3：有关本表的一般注释，见表 A.1 前的正文。
注 4：对于不经常读/写(例如组态过程)的 RAM，若在每次读/写访问之后执行 A.4.1～A.4.4 的措施，则可认为这些措施是有效的。

表 A.7 I/O 单元和接口(外部通信)

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
利用在线监视检测失效	A.1.1	低(低要求模式) 中(高要求或连续模式)	依赖于失效检测的诊断覆盖率
测试模式	A.6.1	高	
代码保护	A.6.2	高	
多通道平行输出	A.6.3	高	仅当诊断测试间隔内数据流改变时才有效
监视输出	A.6.4	高	仅当诊断测试间隔内数据流改变时才有效
输入比较/表决(1oo2,2oo3 或更好的冗余)	A.6.5	高	仅当诊断测试间隔内数据流改变时有效
注 1:本表不取代附录 C 的任何要求。 注 2:附录 C 的要求与诊断覆盖率的确定有关。 注 3:有关本表的一般注释,见表 A.1 前的正文。			

表 A.8 数据路径(内部通信)

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
1 位硬件冗余	A.7.1	低	
多位硬件冗余	A.7.2	中	
完全硬件冗余	A.7.3	高	
使用测试模式进行检查	A.7.4	高	仅对瞬时故障有效
传输冗余	A.7.5	高	
信息冗余	A.7.6	高	
注 1:本表不取代附录 C 的任何要求。 注 2:附录 C 的要求与诊断覆盖率的确定有关。 注 3:有关本表的一般注释,见表 A.1 前的正文。			

表 A.9 电 源

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
使用安全断电或切换到备用电源单元的过压保护	A.8.1	低	应使用本表中的技术,也推荐使用其他技术
使用安全断电或切换到备用电源单元的电压控制(次级)	A.8.2	高	
带安全断电或切换到备用电源单元的断电	A.8.3	高	应使用本表中的技术,也推荐使用其他技术
无功电流原理	A.1.5	低	仅对断电有用
注 1:本表不取代附录 C 的任何要求。 注 2:附录 C 的要求与诊断覆盖率的确定有关。 注 3:有关本表的一般注释,见表 A.1 前的正文。			

表 A.10 程序顺序(看门狗)

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
具有分离时基但无时间窗的看门狗	A.9.1	低	
具有分离时基和时间窗的看门狗	A.9.2	中	
程序顺序的逻辑监视	A.9.3	中	依赖于监视质量
程序顺序的时序和逻辑监视的组合	A.9.4	高	
具有在线检验的时序监视	A.9.5	中	
注 1:本表不取代附录 C 的任何要求。 注 2:附录 C 的要求与诊断覆盖率的确定有关。 注 3:有关本表的一般注释,见表 A.1 前的正文。			

表 A.11 通风和加热系统(若需要)

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
温度传感器	A.10.1	中	
风扇控制	A.10.2	中	
通过热保险丝启动安全断电	A.10.3	高	
来自温度传感器和条件报警的交错报文	A.10.4	高	
强制风冷的连接和状态指示	A.10.5	高	
注 1:本表不取代附录 C 的任何要求。 注 2:附录 C 的要求与诊断覆盖率的确定有关。 注 3:有关本表的一般注释,见表 A.1 前的正文。			

表 A.12 时 钟

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
具有分离时基但无时间窗的看门狗	A.9.1	低	
具有分离时基和无时间窗的看门狗	A.9.2	高	依赖于时间窗的时间限制
程序顺序的逻辑监视	A.9.3	中	仅当外部瞬时事件影响逻辑程序流时才对时钟失效有效
时序和逻辑监视	A.9.4	高	
具有在线检验的时序监视	A.9.5	中	
注 1:本表不取代附录 C 的任何要求。 注 2:附录 C 的要求与诊断覆盖率的确定有关。 注 3:有关本表的一般注释,见表 A.1 前的正文。			

表 A.13 通信和大容量存储器

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
E/E/PE 安全相关系统和过程之间的信息交换	A.6	A.7	见 I/O 单元和接口
E/E/PE 安全相关系统之间的信息交换	A.7	A.8	见数据路径/总线
分隔开电力线和信息线	A.11.1	高	应使用本表中的技术，也推荐使用其他技术
多线路的空间分隔	A.11.2	高	
提高抗干扰性	A.11.3	高	
抗合成信号传输	A.11.4	高	
注 1：本表不取代附录 C 的任何要求。 注 2：附录 C 的要求与诊断覆盖率的确定有关。 注 3：有关本表的一般注释，见表 A.1 前的正文。			

表 A.14 传 感 器

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
利用在线监视检测失效	A.1.1	低(低要求模式) 中(高要求或连续模式)	依赖于失效检测的诊断覆盖率
无功电流原理	A.1.5	低	仅对无需连续控制未达到或保持 EUC 安全状态的 E/E/PE 安全相关系统才有效
模拟信号监视	A.2.7	低	
测试模式	A.6.1	高	
输入比较/表决(1oo2，2oo3 或更好的冗余)	A.6.5	高	仅当诊断测试间隔内数据流改变时才有效
参考传感器	A.12.1	高	依赖于失效检测的诊断覆盖率
可靠启动的开关	A.12.2	高	
注 1：本表不取代附录 C 的任何要求。 注 2：附录 C 的要求与诊断覆盖率的确定有关。 注 3：有关本表的一般注释，见表 A.1 前的正文。			

表 A.15 最终元件(执行器)

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
利用在线监视检测失效	A.1.1	低(低要求模式) 中(高要求或连续模式)	依赖于失效检测的诊断覆盖率
继电器触点监视	A.1.2	高	

表 A.15(续)

诊断技术/措施	见 GB/T 20438.7—2006	经考虑能达到的最大诊断覆盖率	注
无功电流原理	A.1.5	低	仅对无需连续控制来达到或保持 EUC 安全状态的 E/E/PE 安全相关系统有效
测试模式	A.6.1	高	
监视	A.13.1	高	依赖于失效检测的诊断覆盖率
多个执行器的交叉监视	A.13.2	高	
注 1：本表不取代附录 C 的任何要求。 注 2：附录 C 的要求与诊断覆盖率的确定有关。 注 3：有关本表的一般注释，见表 A.1 前的正文。			

A.3 系统安全完整性

表 A.16～表 A.18 给出了有关技术和措施的建议，对应于：

——控制由硬件和软件设计引起的失效(见表 A.16)；

——控制由环境应力或影响引起的失效(见表 A.17)；

——控制操作过程的失效(见表 A.18)。

在表 A.16～表 A.18 中根据安全完整性等级提出的建议首先指明了技术或措施的重要性；其次是使用时要求的有效性。

重要程度表示如下：

——HR：此技术或措施是为该安全完整性等级所极力推荐的。若不使用这种技术或措施，则应详细说明不使用的理由。

——R：此技术或措施是为安全完整性等级所推荐的。至少需要表中浅灰色阴影组中的一项技术。

————：此技术或措施是不推荐或禁止使用的。

——NR：此技术或措施是为该安全完整性等级绝不推荐的。若使用这种技术或措施，则应详细说明使用的理由。

要求的有效性表示如下：

——强制：此技术或措施为所有安全完整性等级所需要，并应尽可能有效地使用(即给出高有效性)。

——低：若使用，采用的技术和措施应在防止系统失效方面至少达到低有效性。

——中：若使用，采用的技术和措施应在防止系统失效方面至少达到中等有效性。

——高：若使用，采用的技术和措施应在防止系统失效方面至少达到高有效性。

表 A.19 为大部分技术和措施的有效性级别提供了指南。

若某项措施为非强制的，那么原则上可被其他措施(单个的或组合的)所代替；这取决于它在表中的色调区域。

这里给出的所有技术和措施均为 E/E/PE 安全相关系统的内在特性，有利于在线控制失效。规程性的和有组织的技术和措施在整个 E/E/PES 安全生命周期中对避免引入故障都是必需的，为证明内在特性适用于具体的应用，需对所采用的技术进行确认，该技术用以测试 E/E/PE 安全相关系统抵御预期的外部影响的行为(见附录 B)。

GB/T 20438.6—2006 的附录 D 给出了共同原因失效的信息。

注：表 A.16～表 A.18 中的大部分措施均可根据表 A.19 在改变有效性的情况下使用，表 A.19 给出了低有效性和高有效性的示例。中等有效性所需的工作介于所规定的低有效性和高有效性的工作之间。

表 A.16 用于控制由硬件和软件设计引起的系统失效的技术和措施

	技术/措施	见 GB/T 20438.7—2006	SIL1	SIL2	SIL3	SIL4
	程序顺序监视	A.9	HR 低	HR 低	HR 中	HR 高
	利用在线监视检测失效(见注 4)	A.1.1	R 低	R 低	R 中	R 高
	利用冗余硬件进行测试	A.2.1	R 低	R 低	R 中	R 高
	访问端口和边界扫描结构的标准测试	A.2.3	R 低	R 低	R 中	R 高
	代码保护	A.6.2	R 低	R 低	R 中	R 高
	多种硬件	B.1.4	— 低	— 低	R 中	R 高
	故障检测和诊断	C.3.1	见 GB/T 20438.3—2006 的表 A.2			
	差错校验和纠错码	C.3.2				
	失效断言编程	C.3.3				
	安全包技术	C.3.4				
	多种程序设计	C.3.5				
	恢复程序块	C.3.6				
	反向恢复	C.3.7				
	正向恢复	C.3.8				
	重试故障恢复机制	C.3.9				
	存储执行用例	C.3.10				
	故障弱化	C.3.11				
	人工智能故障纠正	C.3.12				
	动态再配置	C.3.13				

要求至少应用一种表中浅灰色阴影组中的技术。

注 1：每一安全完整性等级下面表项的含意，应首先查看本表前的正文。

注 2：不涉及 GB/T 20438.3—2006 的表 A.2 的本表中的措施，根据本部分表 A.19 可改变其有效性，表 A.19 给出了低有效性和高有效性的示例。中等有效性所需的工作介于所规定的低有效性和高有效性工作之间。

注 3：GB/T 20438.7—2006 的附录 A、附录 B 和附录 C 给出了与本表相关技术和措施的概述，本表第 2 列为所引用的 GB/T 20438.7—2006 中的有关条款。

注 4：对于在低要求操作模式下工作的 E/E/PE 安全相关系统(例如紧急关闭系统)，通过在线监视由失效检测所达到的诊断覆盖率通常为低或无。

表 A.17　用于控制由环境应力或影响引起的系统失效的技术和措施

	技术/措施	见 GB/T 20438.7—2006	SIL1	SIL2	SIL3	SIL4
	防电压击穿、电压波动、过压、低压的措施	A.8	HR 强制	HR 强制	HR 强制	HR 强制
	分隔开电力线和信息线(见注 4)	A.11.1	HR 强制	HR 强制	HR 强制	HR 强制
	提高抗干扰性	A.11.3	HR 强制	HR 强制	HR 强制	HR 强制
	抗物理环境(如温度、湿度、水、振动、灰尘、腐蚀物)的措施	A.14	HR 强制	HR 强制	HR 强制	HR 强制
	程序顺序监视	A.9	HR 低	HR 低	HR 中	HR 高
	抗温升措施	A.10	HR 低	HR 低	HR 中	HR 高
	多线路的空间分隔	A.11.2	HR 低	HR 低	HR 中	HR 高
	利用在线监视检测失效(见注 5)	A.1.1	R 低	R 低	R 中	R 高
	利用冗余硬件进行测试	A.2.1	R 低	R 低	R 中	R 高
	代码保护	A.6.2	R 低	R 低	R 中	R 高
	抗合成信号传输	A.11.4	R 低	R 低	R 中	R 高
	多种硬件(见注 6)	B.1.4	— 低	— 低	— 中	R 高
	软件结构	GB/T 20438.3—2006 的 7.4.3	见 GB/T 20438.3—2006 的表 A.2			

要求至少应用一种表中浅灰色阴影组中的技术。

注 1：每一安全完整性等级下面表项的含意，应首先查看表 A.16 前的正文。

注 2：本表中的大部分措施可根据表 A.19 用来改变有效性，表 A.19 给出了低有效性和高有效性的示例。中等有效性所需的工作介于所规定的低有效性和高有效性工作之间。

注 3：GB/T 20438.7—2006 的附录 A 和附录 B 给出了与本表相关的技术和措施的概述，本表第二列为所引用的 GB/T 20438.7—2006 中的有关条款。

注 4：若信息传输采用光介质，则无需分离电力线和信息线。并且也不需要分隔开为 E/E/PES 的部件通电，以及载送来自或传送到这些部件的信息而设计的低功率电缆。

注 5：对于在低要求工作模式下工作的 E/E/PE 安全相关系统(例如紧急关闭系统)，通过在线监视由失效检测所达到的诊断覆盖率通常为低或无。

注 6：若通过确认和广泛工作经验证明：为满足目标失效量，硬件充分摆脱了设计故障并足以防止共同原因失效，则不需要多种硬件。

表 A.18 用于控制系统工作失效的技术和措施

	技术/措施	见 GB/T 20438.7—2006	SIL1	SIL2	SIL3	SIL4
	修改保护	B.4.8	HR 强制	HR 强制	HR 强制	HR 强制
	利用在线监视检测失效(见注 4)	A.1.1	R 低	R 低	R 中	R 高
	输入确认	B.4.9	R 低	R 低	R 中	R 高
	失效断言编程	C.3.3	见 GB/T 20438.3—2006 的表 A.2			

要求至少应用一种表中浅灰色阴影组中的技术。

注 1：每一安全完整性等级下面表项的含意，应首先查看表 A.16 前的正文。

注 2：本表中的两项措施可根据表 A.19 改变有效性，表 A.19 给出了低有效性和高有效性的示例。中等有效性所需的工作介于所规定的低有效性和高有效性工作之间。

注 3：GB/T 20438.7—2006 的附录 A、附录 B 和附录 C 给出了与本表相关的技术和措施的概述，本表第二列为所引用的 GB/T 20438.7—2006 中的有关条款。

注 4：对于在低要求操作模式下工作的 E/E/PE 安全相关系统(例如紧急关闭系统)，通过在线监视由失效检测所达到的诊断覆盖率通常为低或无。

表 A.19 控制系统失效的技术和措施的有效性

技术/措施	见 GB/T 20438.7—2006	低有效性	高有效性
利用在线监视检测失效(见注)	A.1.1	EUC 及其控制系统的触发信号用于检查 E/E/PE 安全相关系统的正确工作(仅有时间上限的时间行为)	E/E/PE 安全相关系统由 EUC 及其控制系统的时序信号和逻辑信号再触发(时序看门狗功能的时间窗)
利用冗余硬件进行测试(见注)	A.2.1	附加硬件测试 E/E/PE 安全相关系统的触发信号(仅有时间上限的时间行为)，此硬件可切换备用最终元件	附加硬件由 E/E/PE 安全相关系统的时序和逻辑信号再触发(时序看门狗功能的时间窗)；多通道间的表决
访问端口和边界扫描结构的标准测试	A.2.3	检验测试过程中，通过所定义的边界扫描测试，测试所使用的固态逻辑	根据 E/E/PE 安全相关系统的功能规范进行固态逻辑的诊断测试；对所有集成电路的所有功能进行检验
代码保护	A.6.2	通过信号传输的时间冗余进行失效检测	通过信号传输的时间和信息冗余进行失效检测
程序顺序监视	A.9	程序顺序的时序或逻辑监视	通过程序中的多个检测点进行程序顺序的时序和逻辑监视
抗温升措施	A.10	温度传感器检测超标温度	通过热保险丝触发安全关闭
提高抗干扰性(见注)	A.11.3	电源和临界输入输出处的噪声过滤器；需要时加屏蔽	防止未预期的电磁侵入过滤器；加屏蔽
抗物理环境的措施	A.14	根据应用，通常可接受的惯例	某特殊应用的相关标准中提到的技术

表 A.19(续)

技术/措施	见 GB/T 20438.7—2006	低有效性	高有效性
多种硬件	B.1.4	执行相同功能但设计不同的两个或多个硬件	执行不同功能的两个或多个硬件
输入确认	B.4.9	输入动作返回给操作者的回应	检查操作者输入数据的严格规则,拒收不正确的输入
注:在参考 GB/T 20438.7—2006 中 A.1.1、A.2.1、A.11.3 和 A.14 的技术或措施的情况下,假设用于高有效性的技术和措施也可用于低有效性方案。			

附 录 B
（规范性附录）
用于 E/E/PE 安全相关系统的技术和措施：避免生命周期不同阶段中的系统失效

本附录的表 B.1～表 B.5 推荐了每个安全完整性等级下避免 E/E/PE 安全相关系统失效的技术和措施。有关技术和措施的更多内容可参见 GB/T 20438.7—2006 的附录 B。在工作过程中用来控制失效的措施的要求由附录 A 给出，并在 GB/T 20438.7—2006 的附录 A 中做了描述。

要把整个安全生命周期中出现的系统失效的每个独立原因或每种补救方法都一一列出是不现实的，主要原因有两点：

——系统故障的影响与引入它的生命周期阶段有关；并且

——为避免系统失效的各种单一措施的有效性都与应用有关。

因此，不可能为避免系统失效进行定量分析。

可以根据引入某种原因引起的故障的生命周期阶段，对 E/E/PE 安全相关系统的失效进行分类：

——失效由系统安装之前或系统安装之中的故障诱发（例如，软件故障包括规范和程序故障；硬件故障包括制造故障和部件的不正确选择）；

——失效由系统安装之后的故障诱发（例如：随机硬件失效，或使用不当引起的失效）。

为避免和控制上述情况发生时引起失效，通常需要大量的措施。附录 A 和附录 B 中的要求基于这样一种结构：将测试划分为在工作过程中用来控制失效的那些措施（附录 A），和在 E/E/PE 安全生命周期各阶段中用来避免失效的那些措施（本附录）。虽然是在安全生命周期为避免失效执行措施，但控制失效的措施却是 E/E/PE 安全相关系统的内在特性。

在表 B.1～表 B.5 中根据安全完整性等级提出的建议，首先指明技术或措施的重要性；其次是使用时要求的有效性。

重要程度表示如下：

——HR：此技术或措施是为该安全完整性等级所极力推荐的。若不使用这种技术或措施，则应详细说明不使用的理由。

——R：此技术或措施是为安全完整性等级所推荐的。至少需要表中浅灰色阴影组中的一项技术。

———：此技术或措施是不推荐或禁止使用的。

——NR：此技术或措施是为该安全完整性等级绝不推荐的。若使用这种技术或措施，则应详细说明使用的理由。

要求的有效性表示如下：

——强制：此技术或措施为所有安全完整性等级所需要，并应尽可能有效地使用（即给出高有效性）。

——低：若使用，采用的技术和措施应在防止系统失效方面至少达到低有效性。

——中：若使用，采用的技术和措施应在防止系统失效方面至少达到中等有效性。

——高：若使用，采用的技术和措施应在防止系统失效方面至少达到高有效性。

注：表 B.1～表 B.5 中的大部分措施均可根据表 B.6 在改变有效性的情况下使用，表 B.6 给出了低有效性和高有效性的示例。中等有效性所需的工作介于所规定的低有效性和高有效性工作之间。

若某项措施为非强制的，那么原则上可被其他措施（单个的或组合的）所代替；这取决于它在表中的色调区域。

遵从本附录中的指南不能保证所要求的安全完整性。考虑以下方面是很重要的：

——所选技术和措施的一致性，及其互补性如何；以及

——那项技术和措施适合于生命周期的每个开发阶段；以及

——哪些技术和措施最适合在设计和开发每个特殊的 E/E/PE 安全相关系统中遇到的具体问题。

表 B.1　在 E/E/PES 要求规范中对避免失误的建议(见 7.2)

	技术/措施	见 GB/T 20438.7—2006	SIL1	SIL2	SIL3	SIL4
	项目管理	B.1.1	HR 低	HR 低	HR 中	HR 高
	编制文档	B.1.2	HR 低	HR 低	HR 中	HR 高
	分离开 E/E/PE 安全相关系统与非安全相关系统	B.1.3	HR 低	HR 低	HR 中	HR 高
	结构化规范	B.2.1	HR 低	HR 低	HR 中	HR 高
	规范的检查	B.2.6	— 低	HR 低	HR 中	HR 高
	半形式化方法	B.2.3,也见 GB/T 20438.3—2006 的表 B.7	R 低	R 低	HR 中	HR 高
	检查列表	B.2.5	R 低	R 低	R 中	R 高
	计算机辅助规范工具	B.2.4	— 低	R 低	R 中	R 高
	形式化方法	B.2.2	— 低	— 低	R 中	R 高

表中着灰色阴影组中标记“R”的所有技术均是可替换的,但至少需要其中的一项技术。

为验证此安全生命周期阶段,至少应使用本表或表 B.5 中着灰色阴影组中的一项技术或措施。

注 1:每一安全完整性等级下面表项的含意,应首先查看本表前的正文。

注 2:本表中的措施可根据表 B.6 改变有效性,表 B.6 给出了低有效性和高有效性的示例。中等有效性所需的工作介于所规定的低有效性和高有效性工作之间。

注 3:GB/T 20438.7—2006 的附录 B 给出了与本表相关的技术和措施的概述,本表第二列为所引用的 GB/T 20438.7—2006 中的有关条款。

表 B.2　在 E/E/PES 设计和开发过程中为避免引入故障的建议(见 7.4)

	技术/措施	见 GB/T 20438.7—2006	SIL1	SIL2	SIL3	SIL4
	遵循指南和标准	B.3.1	HR 强制	HR 强制	HR 强制	HR 强制
	项目管理	B.1.1	HR 低	HR 低	HR 中	HR 高
	编制文档	B.1.2	HR 低	HR 低	HR 中	HR 高
	结构化设计	B.3.2	HR 低	HR 低	HR 中	HR 高
	模块化	B.3.4	HR 低	HR 低	HR 中	HR 高

表 B.2(续)

	技术/措施	见 GB/T 20438.7—2006	SIL1	SIL2	SIL3	SIL4
	使用经充分试验过的部件	B.3.3	R 低	R 低	R 中	R 高
	半形式化方法	B.2.3,另见 GB/T 20438.3—2006 的表 B.7	R 低	R 低	HR 中	HR 高
	检查列表	B.2.5	— 低	R 低	R 中	R 高
	计算机辅助设计工具	B.3.5	— 低	R 低	R 中	R 高
	仿真	B.3.6	— 低	R 低	R 中	HR 高
	硬件检查或硬件走查	B.3.7 B.3.8	— 低	R 低	R 中	R 高
	形式化方法	B.2.2	— 低	— 低	R 中	R 高

表中着灰色阴影组中标记"R"的所有技术均是可替换的,但至少需要其中的一项技术。

为验证此安全生命周期阶段,至少应使用本表或表 B.5 中着灰色阴影组中的一项技术或措施。

注 1:每一安全完整性等级下面表项的含意,可查看表 B.1 之前的正文。

注 2:本表中的多项措施可根据表 B.6 改变有效性,表 B.6 给出了低有效性和高有效性的示例。中等有效性所需的工作介于所规定的低有效性和高有效性工作之间。

注 3:GB/T 20438.7—2006 的附录 B 给出了与本表相关的技术和措施的概述,本表第二列为所引用的 GB/T 20438.7—2006 中的有关条款。

表 B.3 在 E/E/PES 集成过程中为避免故障的建议(见 7.5)

	技术/措施	见 GB/T 20438.7—2006	SIL1	SIL2	SIL3	SIL4
	功能测试	B.5.1	HR 强制	HR 强制	HR 强制	HR 强制
	项目管理	B.1.1	HR 低	HR 低	HR 中	HR 高
	编制文档	B.1.2	HR 低	HR 低	HR 中	HR 高
	黑盒测试	B.5.2	R 低	R 低	R 中	R 高
	现场经验	B.5.4	R 低	R 低	R 中	R 高
	统计测试	B.5.3	— 低	— 低	R 中	R 高

表中着灰色阴影组中标记"R"的所有技术均是可替换的,但至少需要其中的一项技术。

为验证此安全生命周期阶段,至少应使用本表或表 B.5 中着灰色阴影组中的一项技术或措施。

注 1:每一安全完整性等级下面表项的含意,可查看表 B.1 之前的正文。

注 2:本表中的多项措施可根据表 B.6 改变有效性,表 B.6 给出了低有效性和高有效性的示例。中等有效性所需的工作介于所规定的低有效性和高有效性工作之间。

注 3:GB/T 20438.7—2006 的附录 B 给出了与本表相关的技术和措施的概述,本表第二列为所引用的 GB/T 20438.7—2006 中的有关条款。

表 B.4　在 E/E/PES 操作和维护规程中为避免故障的建议(见 7.6)

	技术/措施	见 GB/T 20438.7—2006	SIL1	SIL2	SIL3	SIL4
	操作和维护说明书	B.4.1	HR 强制	HR 强制	HR 强制	HR 强制
	用户友善性	B.4.2	HR 强制	HR 强制	HR 强制	HR 强制
	维护友善性	B.4.3	HR 强制	HR 强制	HR 强制	HR 强制
	项目管理	B.1.1	HR 低	HR 低	HR 中	HR 高
	编制文档	B.1.2	HR 低	HR 低	HR 中	HR 高
	有限的操作可能性	B.4.4	— 低	R 低	HR 中	HR 高
	防止操作员出错的措施	B.4.6	— 低	R 低	HR 中	HR 高
	仅可由熟练操作员进行的操作	B.4.5	— 低	R 低	R 中	HR 高

表中着灰色阴影组中标记“R”的所有技术均是可替换的,但至少需要其中的一项技术。

为验证此安全生命周期阶段,应使用检查列表(见 GB/T 20438.7—2006 的 B.2.5)或检查(见 GB/T 20438.7—2006 的 B.2.6)。

注 1:每一安全完整性等级下面表项的含意,应首先查看表 B.1 前的正文。

注 2:本表中的多项措施可根据表 B.6 改变有效性,表 B.6 给出了低有效性和高有效性的示例。中等有效性所需的工作介于所规定的低有效性和高有效性工作之间。

注 3:GB/T 20438.7—2006 的附录 B 给出了与本表相关的技术和措施的概述,本表第二列为所引用的 GB/T 20438.7—2006 中的有关条款。

表 B.5　在 E/E/PES 安全确认过程中为避免故障的建议(见 7.7)

	技术/措施	见 GB/T 20438.7—2006	SIL1	SIL2	SIL3	SIL4
	功能测试	B.5.1	HR 强制	HR 强制	HR 强制	HR 强制
	在环境条件下测试功能	B.6.1	HR 强制	HR 强制	HR 强制	HR 强制
	浪涌抗扰性测试	B.6.2	HR 强制	HR 强制	HR 强制	HR 强制
	故障插入测试(当要求的诊断覆盖率≥90%时)	B.6.10	HR 强制	HR 强制	HR 强制	HR 强制
	项目管理	B.1.1	HR 低	HR 低	HR 中	HR 高
	编制文档	B.1.2	HR 低	HR 低	HR 中	HR 高

表 B.5(续)

	技术/措施	见 GB/T 20438.7—2006	SIL1	SIL2	SIL3	SIL4
	静态分析、动态分析和失效分析	B.6.4 B.6.5 B.6.6	— 低	R 低	R 中	R 高
	仿真和失效分析	B.3.6 B.6.6	— 低	R 低	R 中	R 高
	“最差情况”分析、动态分析和失效分析	B.6.7 B.6.5 B.6.6	— 低	— 低	R 中	R 高
	静态分析和失效分析(见注4)	B.6.4 B.6.6	R 低	R 低	NR	NR
	扩展的功能测试	B.6.8	— 低	HR 低	HR 中	HR 高
	黑盒测试	B.5.2	R 低	R 低	R 中	R 高
	故障插入测试(当所要求的诊断覆盖率<90%时)	B.6.10	R 低	R 低	R 中	R 高
	静态测试	B.5.3	— 低	— 低	R 中	R 高
	“最差情况”测试	B.6.9	— 低	— 低	R 中	R 高
	现场经验	B.5.4	R 低	R 低	R 中	NR

本表分为边条着色指示不同的三个部分,着灰色和着黑色组中所有标记“R”的技术均是可用该组中的其他技术替换的,但至少需要一项着灰色组中的技术(分析技术)和至少需要一项着黑色组中的技术(测试技术)。

注 1:每一安全完整性等级下面表项的含意,应首先查看表 B.1 前的正文。

注 2:本表中的多项措施可根据表 B.6 改变有效性,表 B.6 给出了低有效性和高有效性的示例。中等有效性所需的工作介于所规定的低有效性和高有效性工作之间。

注 3:GB/T 20438.7—2006 的附录 B 给出了与本表相关的技术和措施的概述,本表第二列为所引用的 GB/T 20438.7—2006 中的有关条款。

注 4:对于 SIL3 和 SIL4,不推荐使用静态分析和失效分析,因为,如果不与动态分析结合使用,这些技术并不充分。

表 B.6 避免系统失效的技术和措施的有效性

技术/措施	见 GB/T 20438.7—2006	低有效性	高有效性
项目管理(见注)	B.1.1	行动和责任的定义;进度表编制和资源分配;相关人员培训;修改后的一致性检查	与设计无关的确认;项目监视;标准化的确认规程;配置管理;失效统计;计算机辅助工程;计算机辅助软件工程

表 B.6(续)

技术/措施	见 GB/T 20438.7—2006	低有效性	高有效性
编制文档(见注)	B.1.2	图形和自然语言描述,例如方块图,流程图	整个文档组织的内容和编排相协调的指南;内容检查列表;计算机辅助文档管理,形式化变更控制
分离开 E/E/PE 安全相关系统与非安全相关系统	B.1.3	E/E/PE 安全相关系统和非安全相关系统之间的定义完善的接口	完全将 E/E/PE 安全相关系统与非安全相关系统分离,即非安全相关系统不对安全相关系统进行写访问,并且物理位置是分离开的以避免共同原因的影响
结构化规范	B.2.1	按层次细化至子要求的手册;接口描述	使用计算机辅助工程工具分层细化描述;自动一致性检查;精细到功能级
形式化方法	B.2.2	由有经验的人员使用形式化方法	在类似应用中由有经验的人员借助计算机支持工具使用形式化方法
半形式化方法	B.2.3	用半形式化方法描述关键部分	利用不同的半形式化方法描述整体 E/E/PE 安全相关系统的不同方面,在方法间进行一致性检查
计算机辅助规范工具	B.2.4	不偏好某种特殊设计方法的工具	面向模型的层次结构细分规程;所有对象及其关系的描述;公共数据库;自动的一致性检查
检查列表	B.2.5	为所有安全生命周期阶段准备的检查列表;专注于主要安全问题	为所有安全生命周期阶段准备的详细检查列表
规范的检查	B.2.6	由独立的人进行的安全要求规范检查	由独立组织使用用于纠正所发现的所有故障的正式规程进行检查和复查
结构化设计	B.3.2	人工设计制作的分层电路	已测试电路部分的复用;在规范、设计、电路图和零部件清单中的可追溯性;计算机辅助的;基于已定义的方法(见 7.4.4)
经充分试验过的部件使用(见注)	B.3.3	定尺寸充分富余;构造特性	经使用证实(见 7.4.7.6)
模块化(见注)	B.3.4	尺寸受限的模块;每个模块功能独立	充分证实过的模块的复用;易了解的模块;每个模块最多包含一个输入口、一个输出口和一个失效退出口

表 B.6(续)

技术/措施	见 GB/T 20438.7—2006	低有效性	高有效性
计算机辅助设计工具	B.3.5	安全生命周期复杂阶段的计算机支持	经使用证实(见 7.4.7.6)或已确认的工具的使用;安全生命周期各阶段的通用计算机辅助开发
仿真	B.3.6	基于模块建模,包括外围单元的边界数据	基于部件建模,包括边界数据
硬件的检查	B.3.7	由与设计无关的人进行检查	由独立组织使用用于纠正所发现的所有故障的正式规程进行检查和复查
硬件的走查	B.3.8	走查包括一个与设计无关的人员	走查包括一个独立组织和用于纠正所发现的所有故障的正式规程
受限的操作可能性(见注)	B.4.4	用来控制操作模式变化的按键开关或密码	已定义的允许操作的和健壮的规程
仅可由熟练操作员操作	B.4.5	按被操作的安全相关系统类型进行相关的基本培训,加两年在岗经验	所有操作员的年度培训;每个操作员至少具备 5 年低安全完整性等级的安全设备经验
防止操作员出错(见注)	B.4.6	输入确认	每一输入命令的证实和一致性检查
黑盒测试(见注)	B.5.2	等价类划分测试,边界值测试,使用预先写入的测试用例	根据因果图,结合在极限操作边界的临界状况,执行测试用例
统计测试(见注)	B.5.3	所有输出数据的统计分配	利用工具获得的测试报告;大量测试用例;根据现实应用条件和假设的失效模型得到的输入数据分配
现场经验(见注)	B.5.4	10 000 h 工作时间;具备至少 10 台设备在不同应用中至少一年的经验;统计精确度 95%;未发生安全致命失效	1×10^7 h 工作时间;具备至少 10 台设备在不同应用中至少两年的经验;统计精确度 99.9%;在以往工作中对所有变化(包括不太重要的变化)都详细地编成文档
浪涌抗扰性测试	B.6.2		可证明浪涌干扰性确实高于实际操作环境的边界值
静态分析	B.6.4	基于方块图;亮显暗点;规定测试用例	基于详细图;断定在测试用例过程中预期的行为;使用测试工具

表 B.6(续)

技术/措施	见 GB/T 20438.7—2006	低有效性	高有效性
动态分析	B.6.5	基于方块图;亮显暗点;规定测试用例	基于详细图;断定在测试用例过程中预期的行为;使用测试工具
失效分析	B.6.6	在模块层,包括外围单元的边界数据	在部件层,包括边界数据
最差情况分析	B.6.7	对安全功能实施分析:使用实际工作条件的边界值组合得出该分析	对非安全功能实施分析;使用实际工作条件的边界值组合得出该分析
扩展的功能测试	B.6.8	在由有故障的过程或工况引起的静态输入状态的情况下,还能保持所有安全功能的测试	在由有故障的过程或工况引起的固定输入状态和/或异常输入变化的情况下,都能保持所有安全功能的测试(包括罕见情况)
最差情况测试	B.6.9	在实际工作条件中发现的边界值组合下,仍保持安全功能的测试	在实际工作条件中发现的边界值组合下,仍保持非安全功能的测试
故障插入测试	B.6.10	在子单元级包括边界数据或外围单元	在部件级包括边界数据
注:在参考(GB/T 20438.7—2006 的 B.1.1、B.1.2、B.3.3、B.3.4、B.4.4、B.4.6、B.5.2、B.5.3 和 B.5.4 的技术或措施的情况下,假设用于高有效性的技术和措施也可用于低有效性方案。			

附 录 C
（规范性附录）
诊断覆盖率和安全失效分数

C.1 子系统的诊断覆盖率和安全失效分数的计算

子系统的诊断覆盖率和安全失效分数的计算如下所述：

a) 在不存在诊断测试的情况下进行某种失效模式和效应的分析，以此来确定子系统中的每个部件或组件的每个失效模式对 E/E/PE 安全相关系统行为的影响。提供充足的可用信息（见注 1 和注 2）使之能进行失效模式和效应的分析，从而确立一个足够的与安全完整性要求相称的置信度水平。

注 1：为了进行这种分析，以下信息是必需的：

——E/E/PE 安全相关系统详细方块图，描述子系统以及子系统与 E/E/PE 安全相关系统中可能影响所考虑的安全功能的部分之间的关联。

——描述每一部件或组件以及部件间关连的子系统硬件示意图。

——每个部件或组件的失效模式和失效率以及与安全和危险失效相对应的总失效率的相关百分数。

注 2：本分析所需的严格性依赖于许多因素（见 GB/T 20438.1—2006 的 4.1）。尤其需要考虑所包含的安全功能的安全完整性等级。对于高安全完整性等级，可以预期到，失效模式和效应分析是非常明确的依赖于具体的部件类型和应用环境。同样，对于硬件故障裕度为零的硬件结构中使用的子系统进行彻底和详尽的分析是非常重要的。

b) 根据将导致的结果（不存在诊断测试时）对失效模式进行以下分类：

——安全失效（即：E/E/PE 安全相关系统的安全完整性没有受到损害，例如，失效导致安全关机或对 E/E/PE 安全相关系统的安全完整性没有影响）；

——危险失效（即：导致 E/E/PE 安全相关系统或系统的部分丧失功能或导致 E/E/PE 安全相关系统的安全完整性产生了不同方式的损害）。

c) 通过对每一部件或组件的失效概率 λ 的估算（见注 2 和注 3），以及失效模式和效应的分析结果，计算出各部件或组件的安全失效概率 λ_S 和危险失效概率 λ_D。

注 3：每一部件或组件的失效概率是在一个比较短的时段 t 内发生失效的概率。在 λ_t 的值远小于 1 的情况下，它可以被等同于单位时间 t 内的失效率 λ。

注 4：使用来自公认的工业源数据，并考虑应用环境因素，估算每一部件或组件的失效率。但最好还是使用具体应用的数据，特别是在子系统包含较少数量的部件的情况下，以及在估算某个特定部件的安全和危险失效概率过程中出现的任何错误会对安全失效分数的计算产生重大影响的情况下。

d) 对每一部件或组件，估算诊断测试（见 C.2）检测到的危险失效分数，并因此计算诊断测试检测到的危险失效概率 λ_{DD}。

e) 对于子系统，计算危险失效总概率 $\Sigma\lambda_D$，诊断测试检测到的危险失效总概率 $\Sigma\lambda_{DD}$，以及安全失效总概率 $\Sigma\lambda_S$。

f) 计算子系统的诊断覆盖率 $\Sigma\lambda_{DD}/\Sigma\lambda_D$。

g) 计算子系统安全失效分数 $(\Sigma\lambda_S+\Sigma\lambda_{DD})/(\Sigma\lambda_S+\Sigma\lambda_D)$。

注 5：在计算随机硬件失效概率（见 7.4.3.2.2）时，应考虑 E/E/PE 安全相关系统的每一子系统的诊断覆盖率（如有的话）。在确定硬件安全完整性的结构约束时（见 7.4.3.1），应考虑安全失效分数。

用于确定诊断覆盖率和安全失效分数的分析应包括所有的部件，包括：电气的、电子的、机电的、机械的等，这些部件是确保子系统按 E/E/PE 安全相关系统要求的那样处理安全功能所必需的。对于每个部件应考虑所有可能导致某种非安全状态的危险失效模式（当要求响应时阻止这种安全响应）或对

E/E/PE 安全相关系统的安全完整性的其他损害。

表 A.1 提供了为达到有关的诊断覆盖率最低限度应检测到的或者在确定安全失效分数时最低限度应包含的故障或失效。如果使用现场数据来支持失效模式和效应的分析，现场数据应足以支持安全完整性的要求。在统计学上，最低限度单边置信度下限至少要求达到 70%。

注 6：在 GB/T 20438.6—2006 的附录 C 中，包含了一个计算诊断覆盖率和安全失效分数的示例。

注 7：计算诊断覆盖率的一些替代方法包括如使用含有 E/E/PE 的安全相关系统设计中所用的 E/E/PE 安全相关系统的电路及部件的计算机模型(例如在集成电路中细化到晶体管层)的故障仿真。

C.2 确定诊断覆盖率的各种因素

在计算某个子系统的诊断覆盖率(见 C.1)时，必需估算由诊断测试检测到的每个部件或组件的危险失效分数。对诊断覆盖率有贡献的诊断测试包括(但不限于)：

——比较检验，例如监测和比较冗余信号；

——附加内部测试例行程序，例如内存的校验和；

——外部激励测试，例如通过控制路径发送一个脉冲信号；

——某个模拟信号的连续监测，例如检测指示传感器失效的超量程值。

为了计算诊断覆盖率，必需确定诊断测试检测到的那些失效模式。对简单部件(电阻器、电容器、晶体管等)而言，检测开路或短路的失效覆盖率可达 100%。而对较复杂的 B 类部件(见 7.4.3.1.3)，就应考虑到对表 A.1 所示的各种部件的诊断覆盖率的限制。对子系统的每个部件或组件以及对 E/E/PE 的安全相关系统的每个子系统都应执行这种分析。

注 1：表 A.2～表 A.15 为诊断测试推荐了一些技术和措施，并推荐了能声明的最大诊断覆盖率。可以连续或定期(依赖于诊断测试间隔)进行这些测试。这些表并不取代附录 C 的要求。

注 2：在达到 E/E/PE 的安全相关系统的功能安全中，诊断测试可提供相当大的好处。但一定要注意不要增加不必要的复杂性，例如这种情况可能使得执行验证、确认、功能安全评估、维护和修改活动的难度加大。复杂性的增加也可使长期保持 E/E/PE 安全相关系统的功能安全更加困难。

注 3：为获得诊断覆盖率所进行的计算和所用的方法假设当出现其他危险故障时，E/E/PE 安全相关系统仍可安全运行，且此故障可被诊断测试检测到。如此假设不成立，则应认为 E/E/PE 安全相关系统是在高要求(或)连续模式下工作的(见 7.4.6.3 和 7.4.3.2.5)。

注 4：GB/T 20438.4—2006 的 3.8.6 给出了诊断覆盖率的定义，重要的是要注意有时假设了诊断覆盖率的一些替代定义，不过它们并不适用。

注 5：可由 E/E/PE 安全相关系统中的另一子系统来实现用于检测某个子系统中的危险失效的诊断测试。

注 6：既可以连续地也可以定期地(依赖于诊断测试间隔)进行诊断测试。由于有可能对系统状态产生不利的影响，在有些情况下和有的时候不能运行诊断测试。

参 考 文 献

[1] IEC 61000-4 电磁兼容性 第4部分:测试和测量技术.
[2] IEC 60870-5-1:1990 遥控设备和系统 第5部分:传输协议 第1篇:传输帧格式.
[3] IEC 61164:1995 可靠性发展历程 统计测试和估算方法.
[4] EN 50159-1 铁路应用 封闭式传输系统中的安全通信.
[5] EN 50159-2 铁路应用 开放式传输系统中的安全通信.
[6] ANSI/ISA-S84.01:1996 装有安全仪表的系统在过程工业中的应用.
[7] ANSI/IEEE-std 352:1987 核电站安全相关系统可靠性分析的一般原理的IEEE指南.

GB/T 20438.2—2006/IEC 61508-2:2000

中 华 人 民 共 和 国
国 家 标 准
电气/电子/可编程电子安全相关系统的
功能安全 第2部分:电气/电子/
可编程电子安全相关系统的要求
GB/T 20438.2—2006/IEC 61508-2:2000
*
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 3.5 字数 99 千字
2007年2月第一版 2007年2月第一次印刷
*
书号:155066·1-28707 定价 22.00 元

GB/T 20438.2-2006