ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.2—2017/IEC 61508-2:2010
代替 GB/T 20438.2—2006

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 61508-2:2010,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

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2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 20438.2—2006《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》，与GB/T 20438.2—2006相比，主要技术变化如下：

——增加了ASIC开发生命周期(见图3)；

——增加了符合项的安全手册(见附录D)。

本部分使用翻译法等同采用IEC 61508-2:2010《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》。

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：由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、皮尔磁工业自动化贸易(上海)有限公司、上海工业自动化仪表研究院、北京和利时系统工程有限公司、欧姆龙自动化(中国)有限公司、西门子(中国)有限公司、上海中沪电子有限公司。

本部分主要起草人：史学玲、田雨聪、冯晓升、黄之炯、张艾森、郑威、周有铮、华镕、罗安、熊文泽、杨柳、李佳、梅豪、周纯杰、徐皑冬、钱大涛、孟邹清、刘瑶、王德吉。

本部分所代替标准的历次版本发布情况为：

——GB/T 20438.2—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，将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宜具有高度一致性（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 的本部分

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、电子或可编程电子组件;

c) 适用于 E/E/PE 安全相关系统中的所有组件(包括传感器、执行器和操作员界面);

d) 规定了如何按照 GB/T 20438.1 定义的 E/E/PE 系统安全要求规范(由 E/E/PE 系统安全功能要求规范和 E/E/PE 系统安全完整性要求规范组成),开发出 E/E/PE 系统设计要求规范;

e) 规定了在 E/E/PE 安全相关系统的设计和制造过程中(即建立 E/E/PE 系统安全生命周期模型)除软件外所进行活动的要求,软件要求在 GB/T 20438.3(见图 2～图 4)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、调试以及最终安全确认所需的信息;

g) 不适用于 E/E/PE 安全相关系统的运行和维护阶段,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 安全相关系统的运行和维护所需的信息和规程的准备要求;

h) 规定了对 E/E/PE 安全相关系统进行各种修改的各方应满足的要求;

注 1:本部分主要直接面向供应商和/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 4。

i) 不适用于符合 IEC 60601 的医疗设备。

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,虽然它不是针对低复杂的 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 各技术委员会的责任之一,是在其标准的起草工作中尽可能使用基础的安全标准。在本部分中,本基础安全标准中的要求、测试方法或测试条件只有在这些技术委员会起草的标准中已明确引用或包含时适用。

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,认真考虑和充分引用所有相关要求是十分重要的。

1.4 图 1 表示了 GB/T 20438 的整体框架,同时指出了本部分在实现 E/E/PE 安全相关系统的功能安全过程中的作用。GB/T 20438.6—2017 的附录 A 详述了 GB/T 20438.2 和 GB/T 20438.3 的应用。

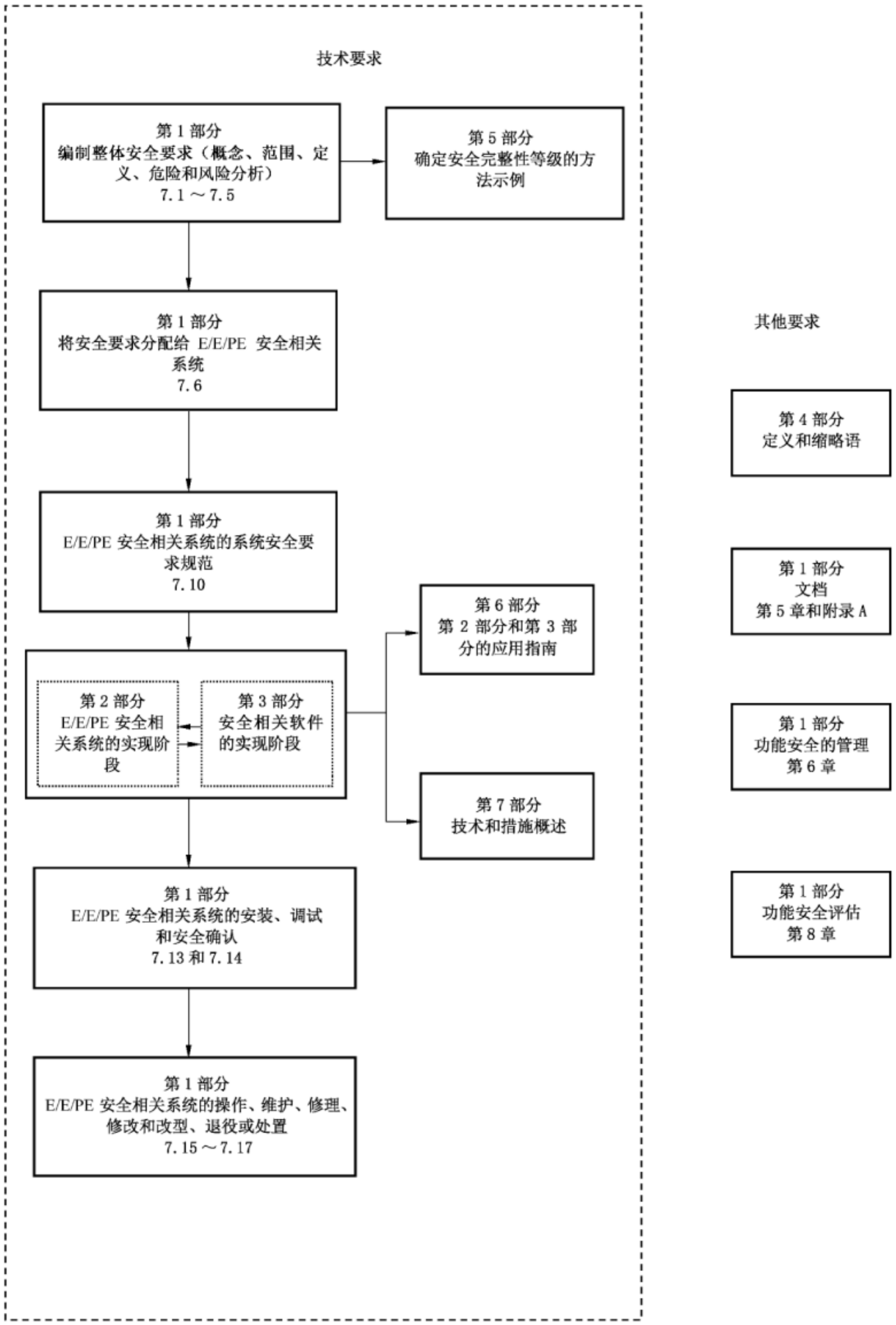


图 1　GB/T 20438 的整体框架

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 20438.1—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(IEC 61508-1：2010，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)

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(IEC 61508-7：2010，IDT)

IEC 60947-5-1 低压开关设备和控制设备 第5-1部分：控制电路电器和开关元件 机电式控制电路电器(Low-voltage switchgear and controlgear—Part 5-1：Control circuit devices and switching elements—Electromechanical control circuit devices)

IEC/TS 61000-1-2 电磁兼容性(EMC)第1-2部分：通则 电气和电子系统包括带有电磁现象设备的功能安全实现方法(Electromagnetic compatibility (EMC)—Part 1-2：General—Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena)

IEC 61326-3-1 测量、控制和实验室用的电设备 电磁兼容性要求 第3-1部分：对于安全相关系统和打算执行安全相关功能(功能安全)设备的免疫要求 通用工业应用(Electrical equipment for measurement，control and laboratory use—EMC requirements—Part 3-1：Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety)—General industrial applications)

IEC 61784-3 工业通信网络 行规 第3部分：功能安全现场总线 通用规则和行规定义(IEC 61784-3，Industrial communication networks—Profiles—Part 3：Functional safety fieldbuses—General rules and profile definitions)

IEC 62280-1 轨道交通 通信、信号和处理系统 第1部分：封闭式传输系统中的安全相关通信(Railway applications—Communication，signalling and processing systems—Part 1：Safety-related communication in closed transmission systems)

IEC 62280-2 轨道交通 通信、信号和处理系统 第2部分：开放式传输系统中的安全相关通信(Railway applications—Communication，signalling and processing systems—Part 2：Safety-related communication in open transmission systems IEC Guide 104：1997，The preparation of safety publications and the use of basic safety publications and group safety publications)

IEC Guide 104：1997 安全出版物的编写及基础安全出版物和多专业共用安全出版物的应用导则(The preparation of safety publications and the use of basic safety publications and group safety publications)

ISO/IEC Guide 51：1999 涉及安全的内容 将安全内容纳入标准的指南(Safety aspects—Guidelines for their inclusion in standards)

EN 50205 带强制继电器导向(机械链接)触点(Relays with forcibly guided (mechanically linked) contacts)

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。

4 与 GB/T 20438 的符合性

本部分对 GB/T 20438 的符合性要求，详见 GB/T 20438.1—2017 的第 4 章。

5 文档

本部分对文档的要求，详见 GB/T 20438.1—2017 的第 5 章。

6 功能安全管理

本部分对功能安全管理的要求，详见 GB/T 20438.1—2017 的第 6 章。

7 E/E/PE 系统安全生命周期要求

7.1 概述

7.1.1 目的和要求：概述

7.1.1.1 7.1 阐述 E/E/PE 系统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/PE 系统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 7.1 的第一个目的是以系统化的方式构造应考虑的 E/E/PE 系统安全生命周期的各阶段，以实现 E/E/PE 安全相关系统所需的功能安全。

7.1.2.2 7.1 的第二个目的是将贯穿于 E/E/PE 系统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建立文档。

7.1.3 要求

7.1.3.1 用来声明符合 GB/T 20438 的 E/E/PE 系统安全生命周期如图 2 所示。用于 ASIC 设计(见 GB/T 20438.4—2017 的 3.2.15)的 ASIC 开发生命周期的一个详细的 V 模型如图 3 所示。如果采用其他 E/E/PE 系统安全生命周期或 ASIC 开发生命周期，则应作为功能安全活动管理的一部分(见 GB/T 20438.1—2017 第 6 章)加以说明，并应满足 GB/T 20438.2 所有条款的目的和要求。

注 1：GB/T 20438.2 和 GB/T 20438.3 之间的关系和范围见图 4。

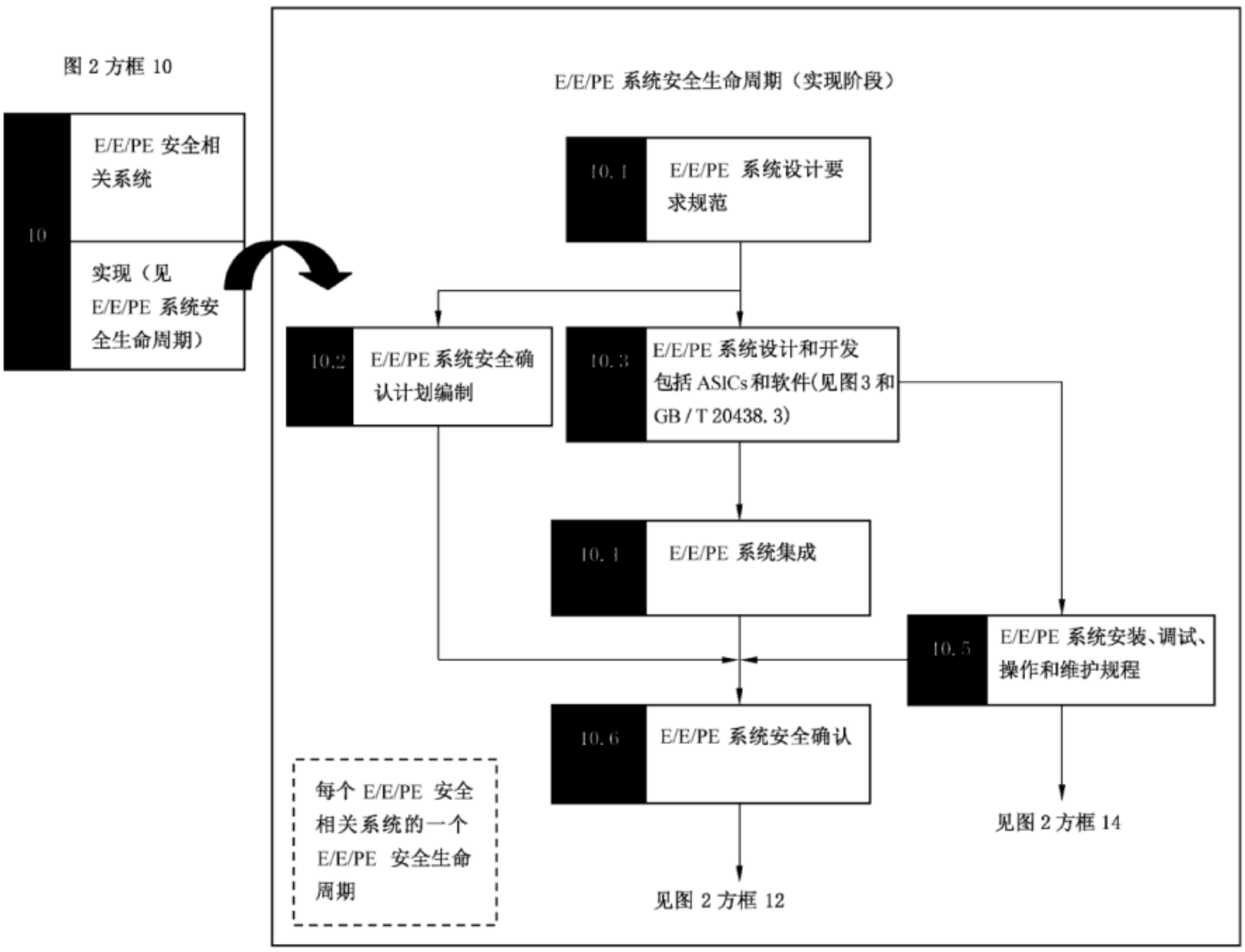
注 2：ASIC 和软件的设计流程非常相似。GB/T 20438.3 建议设计安全相关软件时采用 V 模型。V 模型要求有一个清晰的结构化设计流程和模块化软件结构，以避免和控制系统性故障。ASIC 设计（如图 3 所示）的开发生命周期遵照这个模型。首先由系统要求导出 ASIC 规范，依次是 ASIC 架构、ASIC 设计和模块设计。V 模型左侧的每一步的结果都是下一步的输入，并且在适当的地方返回到之前的步骤构成迭代，直到最后的代码生成。通过布局后仿真、模块测试、模块集成测试和完整 ASIC 验证来验证代码符合相应阶段的设计。任何一步的结果都可能迫使之前的步骤进行修正。最终，在集成到 E/E/PE 安全相关系统后，确认 ASIC。

7.1.3.2　功能安全的管理规程（见 GB/T 20438.1—2017 的第 6 章）应与 E/E/PE 系统安全生命周期的各阶段并行。

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

7.1.3.4　除非判定为是功能安全活动管理的一部分（参见 GB/T 20438.1—2017 的第 6 章），否则 E/E/PE 系统安全生命周期的每个阶段的输出都应建立文档（参见 GB/T 20438.1—2017 的第 5 章）。

7.1.3.5　E/E/PE 系统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）。



注 1：另见 GB/T 20438.6—2017 的附录 A.2b）。

注 2：这个图只展示了在整体安全生命周期实现阶段中的 E/E/PE 系统安全生命周期阶段。完整的 E/E/PE 系统安全生命周期还包含整体安全生命周期（GB/T 20438.1—2017 中图 2 的方框 12～16）有关 E/E/PE 安全相关系统的后续阶段。

图 2　E/E/PE 系统安全生命周期（实现阶段）

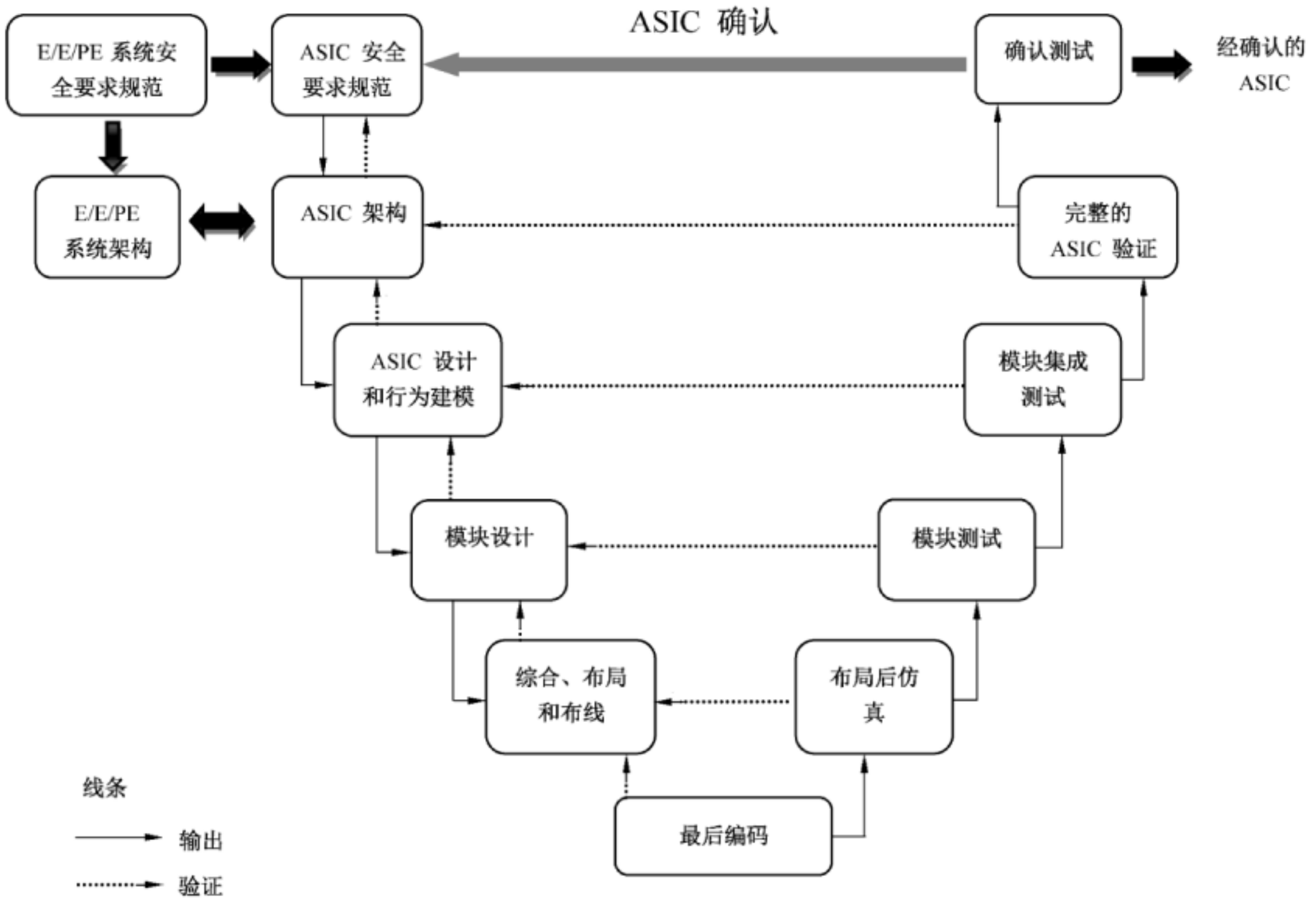


图 3　ASIC 开发生命周期(V 模型)

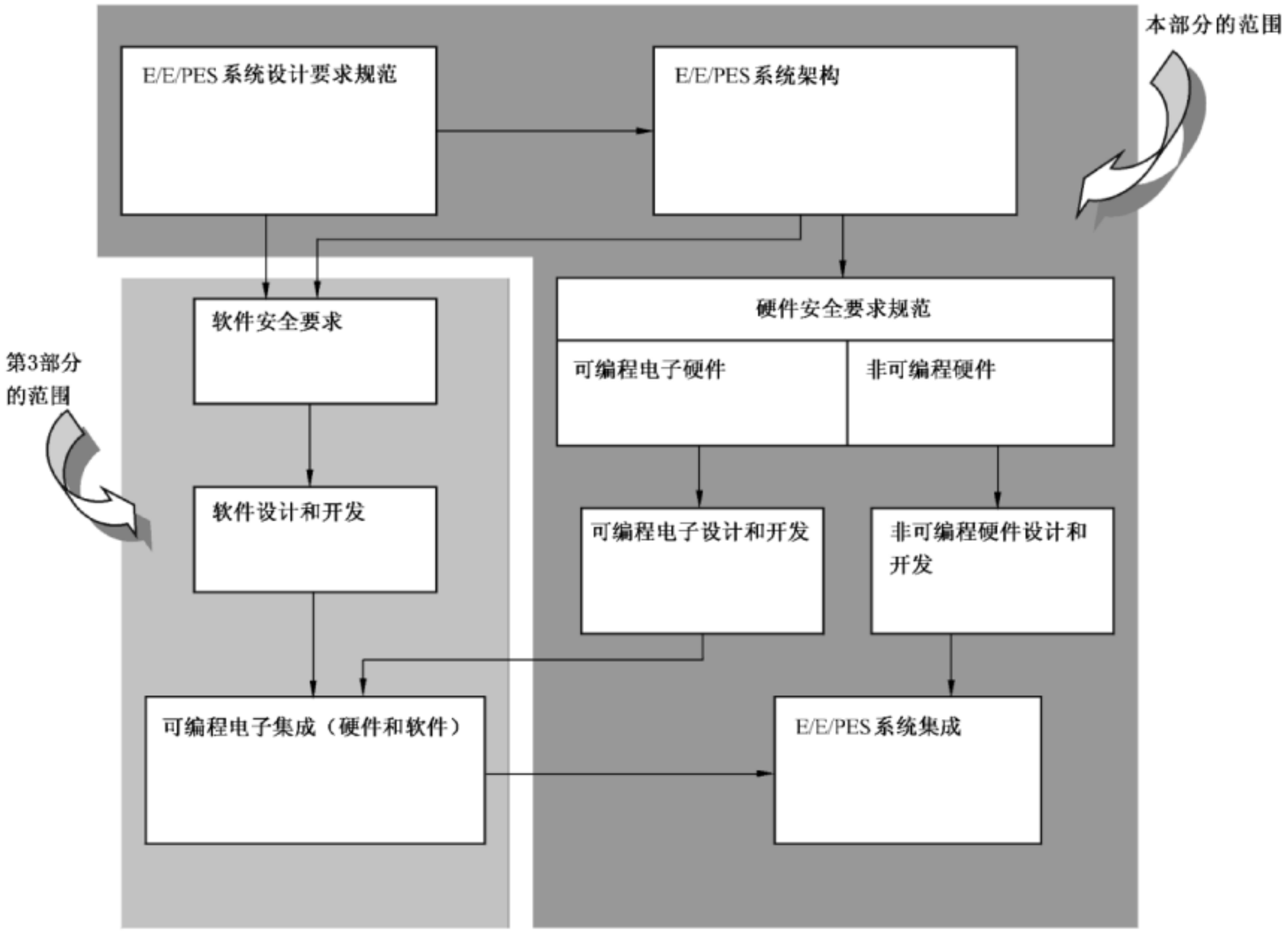


图 4　GB/T 20438.2 和 GB/T 20438.3 的范围和关系

表 1　E/E/PE 系统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					
10.1	E/E/PE 系统设计要求规范	规定每个 E/E/PE 安全相关系统的设计要求，包括子系统和组件。(见 GB/T 20438.1—2017 中 7.10.2)	E/E/PE 安全相关系统	7.2.2	E/E/PE 系统安全要求规范(见 GB/T 20438.1—XXXX 中 7.10)	E/E/PE 系统设计要求规范，描述 E/E/PE 系统的设备和架构
10.2	E/E/PE 系统安全确认计划编制	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/PE 系统安全要求规范和 E/E/PE 系统设计要求规范	E/E/PE 安全相关系统的安全确认计划
10.3	E/E/PE 系统设计和开发，包括 ASIC 和软件(见图 3 和 GB/T 20438.3)	设计和开发满足 E/E/PE 系统设计要求规范(与安全功能要求和安全完整性要求有关(见 7.2))的 E/E/PE 安全相关系统(可能包含 ASIC)	E/E/PE 安全相关系统	7.4.2～7.4.11	E/E/PE 系统设计要求规范	符合 E/E/PE 系统设计要求规范的 E/E/PE 安全相关系统设计； E/E/PE 系统集成测试计划； 作为软件要求规范输入的 PE 系统架构信息
10.4	E/E/PE 系统集成	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/PE 系统设计； E/E/PE 系统集成测试计划； 可编程电子硬件和软件	符合 E/E/PE 系统设计的全功能的 E/E/PE 安全相关系统； E/E/PE 系统集成测试的结果
10.5	E/E/PE 系统安装、调试、运行和维护规程	拟定规程以保证 E/E/PE 安全相关系统在运行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/PE 系统设计要求规范；E/E/PE 系统设计	各个 E/E/PE 系统单独安装、调试、运行和维护的规程
10.6	E/E/PE 系统安全确认	确认 E/E/PE 安全相关系统在各个方面都满足基于所需的安全功能和所需的安全完整性的安全要求	E/E/PE 安全相关系统	7.7.2	E/E/PE 系统安全要求； E/E/PE 系统设计要求规范； 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/PE 系统安全确认结果
—	E/E/PE 系统修改	改正、增强或适应性修改 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/PE 系统设计要求规范	E/E/PE 系统修改结果

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					
—	E/E/PE 系统验证	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/PE 系统功能安全评估	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/PE 系统功能安全评估计划	E/E/PE 系统功能安全评估结果

7.2 E/E/PE 系统设计要求规范

注：这一阶段是图 2 的方框 10.1。

7.2.1 目的

7.2 的目的是为实现所需的功能安全，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、子系统和组件的设计要求。

注：通过将安全功能分解并将分解后的各部分分配到子系统中去（如传感器组，逻辑解算器或执行器），E/E/PE 系统设计要求规范一般取决于 E/E/PE 系统安全要求规范。对子系统的要求可能包含在 E/E/PE 系统设计要求规范中或是独立的并引自 E/E/PE 系统设计要求规范。子系统可能被分解成组件或架构来满足 7.4 的设计和开发要求。对这些组件的要求可能包含在对子系统的要求中，也可能是独立的并引自子系统的要求。

7.2.2 概述

7.2.2.1 E/E/PE 系统设计要求规范应来源于在 GB/T 20438.1—2017 的 7.10 中规定的 E/E/PE 系统安全要求规范。

注：如果同一套 E/E/PE 安全相关系统既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。另见 7.4.2.3。

7.2.2.2 E/E/PE 系统的设计要求规范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；

b) 文字便于在 E/E/PE 系统安全生命周期任一阶段采用信息的各方理解；

c) 可追溯到 E/E/PE 系统安全要求规范。

7.2.3 E/E/PE 系统设计要求规范

7.2.3.1 E/E/PE 系统设计要求规范应包括与安全功能（见 7.2.3.2）和完全完整性（见 7.2.3.3）相关的设计要求。

7.2.3.2 E/E/PE 系统设计要求规范应该包括执行要求的安全功能所必需的所有软硬件的详细信息，这些安全功能是在 E/E/PE 系统安全功能要求规范中（见 GB/T 20438.1—2017 的 7.10.2.6）规定的，针对每个安全功能，规范应包括：

a) 子系统及与它们的软硬件组件相应的要求；
b) 子系统集成的要求及满足 E/E/PE 系统安全功能要求规范的软硬件组件的要求；
c) 能够满足响应时间要求的吞吐量性能；
d) 测量和控制的准确性和稳定性要求；
e) E/E/PE 安全相关系统和操作员接口；
f) E/E/PE 安全相关系统和任何其他系统的接口(与 EUC 关联的外部接口或内部接口)；
g) E/E/PE 安全相关系统的所有行为模式——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、自动停车等)；
h) 所有硬件或软件相互作用的重要性和与软硬件相关的任何要求的约束；

注：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 安全相关系统及其有关的组件的限制与约束条件，例如：时序约束或者由可能的共因失效带来的约束；
j) 启动和重启 E/E/PE 安全相关系统的有关规程的任何特定要求。

7.2.3.3 E/E/PE 系统设计要求规范应该包含与设计相关的详细资料，以实现在 E/E/PE 系统安全完整性要求规范(见 GB/T 20438.1—2017 的 7.10.2.7)中规定的安全功能的安全完整性等级和所需的目标失效量，包括：

a) 每个子系统的架构，该架构应满足硬件安全完整性的架构约束(见 7.4.4)；
b) 所有相关的可靠性建模参数，比如满足目标失效量所需的所有硬件组件的检验测试频率；

注 1：要考虑特定应用的信息(见 GB/T 20438.1—2017 的 7.10.2.1)。这对维护至关重要，规定的检验测试时间间隔不宜小于特定应用的合理期望值。例如，为公共使用的大批量生产的产品的现实可实现的服务间隔时间可能比受控较多的应用的时间要长。

c) 诊断发现危险失效时所采取的行动；
d) 使 E/E/PE 硬件检验测试得以实施的要求、约束、功能与设施；
e) E/E/PE 系统的安全生命周期中，包括制造、贮存、运输、测试、安装、调试、运行和维护，设备满足极端环境条件(例如：温度、湿度、机械的、电气的)的能力；
f) 要求的抗电磁干扰等级(见 IEC/TS 61000-1-2:2008)；

注 2：安全相关系统不同组件所需的抗干扰等级可能变化，其取决于物理位置和供电布局。

注 3：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更严酷的电磁环境下使用或装在某些特殊的位置时，可能有必要使用高于这些标准中规定的抗干扰等级或增加额外的抗干扰要求。

g) 安全管理必需的质量保证或质量控制措施(GB/T 20438.1—2017 中 6.2.5)。

7.2.3.4 E/E/PE 系统设计要求规范应随着设计过程在细节上逐步完善，并在修改后进行必要的更新。

7.2.3.5 为了在 E/E/PE 系统设计要求规范的编制中避免错误，应根据表 B.1 采用一组适当的技术和措施。

7.2.3.6 要考虑 E/E/PE 系统设计要求中隐含的对架构的强制要求。

注：宜包括对达到要求的安全完整性的实现方式简单性的考虑(包括架构的考虑，以及功能分配到组态数据或嵌入式系统)。

7.3 E/E/PE 系统安全确认计划编制

注：这一阶段是图 2 的方框 10.2。它通常与 E/E/PE 系统设计和开发并行(见 7.4)。

7.3.1 目的

7.3 的目的是编制 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 编制计划以便规定步骤(包括规程和技术),用于证明 E/E/PE 安全相关系统满足 E/E/PE 系统安全要求规范(见 GB/T 20438.1—2017 的 7.10)和 E/E/PE 系统设计要求规范(见 7.2)。

7.3.2.2 编制 E/E/PE 安全相关系统的确认计划应考虑以下几条:

a) E/E/PE 系统安全要求规范和 E/E/PE 系统设计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,包括所有必需的工具和设备(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:对安全相关系统组件抗电磁干扰测试规范的指南在 IEC/TS 61000-1-2 中给出。

g) 解决确认未通过的方针。

7.4 E/E/PE 系统的设计与开发

注:这一阶段是图 2 的方框 10.3,它通常与 E/E/PE 系统安全确认计划编制并行(见 7.3)。

7.4.1 目的

7.4 的目的是设计和开发 E/E/PE 安全相关系统(可能包括 ASIC,见 GB/T 20438.4—2017 的 3.2.15)以满足 E/E/PE 系统设计要求规范(与安全功能要求和安全完整性要求一致)(见 7.2)。

7.4.2 一般要求

7.4.2.1 根据 E/E/PE 系统设计要求规范(见 7.2.3)设计 E/E/PE 安全相关系统,应考虑 7.2.3 的所有要求。

7.4.2.2 E/E/PE 安全相关系统(包括整体硬件和软件架构、传感器、执行器、可编程电子、ASIC、嵌入式软件、应用软件和数据等)的设计,应该满足下面 a)~e)的所有要求:

a) 硬件安全完整性要求包括:

——硬件安全完整性的架构约束(见 7.4.4);

——量化随机失效影响的要求(见 7.4.5)。

b) 对带片上冗余集成电路的特殊架构要求(见附录 E),除非可以证明,使用了一组不同于附录 E 的措施能够实现不同通道间具有相同水平的独立性。

c) 系统性安全完整性(系统性能力)要求,可通过实现以下合规路线之一来满足:

——路线 1_S:符合避免系统性故障要求(见 7.4.6 和 GB/T 20438.3)和控制系统性故障要求(见 7.4.7 和 GB/T 20438.3);

——路线 2_S:符合设备经使用证明的要求(见 7.4.10);

——路线 3_S(仅针对已有软件组件):符合 GB/T 20438.3—2017 的 7.4.2.12 的要求。

注:以上路线的下标"S"指系统性安全完整性,以将它和硬件安全完整性的路线 1_H,路线 2_H 区分开。

d) 检测到故障时系统行为要求(见 7.4.8)。

e) 数据通信过程要求(见 7.4.11)。

7.4.2.3 当 E/E/PE 安全相关系统既执行安全功能又执行非安全功能时,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:非安全和安全相关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 系统安全生命周期活动（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，在设计期间应对以下几条建立文档：

a） 达到独立的方法；

b） 方法的合理性证明。

示例：利用 FMECA 或者相关失效分析，找出可预见的可能影响独立性的失效模式和失效率。

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 系统的开发者应特别考虑以下几条：

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/PE 系统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，为满足要求的安全完整性等级所选择技术和措施形成的集合的合理性。

注：对 E/E/PE 安全相关系统（包括传感器、执行器等）采用经过独立型式认可的硬件和软件、诊断测试和编程工具，以及使用适当的编程语言，都有降低 E/E/PE 系统应用工程的复杂性的潜力。

7.4.2.10 在设计与开发活动中，应对所有软硬件相互作用的重要程度（如相关）进行识别、评价并建立文档。

7.4.2.11 设计应基于子系统分解的方法，每一个子系统有特定的设计和一套集成测试（见 7.5.2）。

注 1：单个组件或任意一组组件都可以认为是一个子系统。子系统定义参见 GB/T 20438.4。一个完整的 E/E/PE 安全相关系统是由若干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 7.4.9.3 和 7.4.9.4）。

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：即现有子系统的功能、能力、性能几乎能够 100％的映射于新要求上；或是已验证过的子系统由这样一种方式组成，即用户仅能选择特定应用所需的功能、能力和性能。如果现有子系统或组件被做得太复杂，或是具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 在 E/E/PE 安全相关系统的初步设计完成后，应进行分析以确定是否有任何合理可预见的 E/E/PE 安全相关系统的失效可能导致危险的情况，或对任何其他风险控制措施的要求。如果任何合理可预见的失效会导致上述情况，那么首要任务应改变 E/E/PE 安全相关系统的设计，以避免此类的失效模式，否则，应采取措施将此类失效模式的可能性降低到和目标失效量一样的水平，这些措施应当符合 GB/T 20438 提出的要求。

注：该条款的目的是要找出 E/E/PE 安全相关系统产生对其他风险控制措施要求的失效模式，当特定的失效模式的失效率无法降低时，将要求一个新的安全功能，或者根据失效率重新考虑其他安全功能的 SIL。

7.4.2.13 所有硬件元件应考虑降额（见 GB/T 20438.7）使用。在其极限值下使用硬件元件的合理性证

明应建立文档(见 GB/T 20438.1—2017 的第 5 章)。

注:在使用降额的情况下,降额因子的典型值约为三分之二。

7.4.2.14 在 E/E/PE 安全相关系统设计中,如包括一片或者多片执行安全功能的 ASIC,应使用 ASIC 开发生命周期(见 7.1.3.1)。

7.4.3 组合组件以实现要求的系统性能力

7.4.3.1 在本条描述的情况中,为满足对系统性安全完整性的要求,指定的安全相关 E/E/PE 系统可能被分割为不同系统性能力的组件。

注 1:组件的系统性能力决定了该组件导致安全功能失效的系统性故障的可能性。系统性能力的概念可用于硬件和软件组件。

注 2:GB/T 20438.1—2017 中 7.6.2.7 指出了独立性与多样性在安全功能和具有该安全功能的 E/E/PE 安全相关系统层面的价值。这些概念也适用于详细设计层面,多个具有安全功能的组件组合在一起的系统性能力可能优于单个组件。

7.4.3.2 对于某具有系统性能力 SC N (N=1, 2, 3)的组件,若该组件的系统性故障并不会使指定安全功能失效,而仅在另一个具有系统性能力 SC N 的组件同时发生系统故障时才会使指定功能失效,则在两个组件之间足够独立的前提下其组合的系统性能力可视为 SC (N+1)(见 7.4.3.4)。

注:评价组件的独立性的前提是已知这些组件在确定的安全功能方面的具体应用。

7.4.3.3 多个系统性能力为 SC N 的组件组合后可声明的最高系统性能力为 SC(N+1)。每个 SC N 组件在这种方式下仅能使用一次,不允许继续增加 SC N 组件达到或超过 SC (N+2)。

7.4.3.4 应通过共因失效分析判断,在设计中和在应用中组件间有足够的独立性,确保各组件间以及组件与环境之间的干扰远低于所考虑的安全功能的安全完整性等级。

注 1:针对系统性能力,在硬件设计、实现、运行与维护方面获得充分独立性的可能的措施包括:

——功能多样性:使用不同的方法实现相同的结果;

——多样化的技术:使用不同类型的设备实现相同的结果;

——共用部件/服务:确保不存在其失效会导致整个系统进入危险失效模式的某个共用部件或服务或支持系统(如电源);

——共用规程:确保没有共用的运行、维护或测试规程。

注 2:应用独立性意味着组件不会由于彼此影响的执行动作而导致发生危险失效。

注 3:软件组件的独立性见 GB/T 20438.3—2017 中 7.4.2.8 和 7.4.2.9。

7.4.4 硬件安全完整性架构约束

注 1:与硬件安全完整性约束相关的公式在附录 C 中规定,并且安全完整性约束在表 2 和表 3 中给出。

注 2:GB/T 20438.6—2017 中 A.2 给出了实现所需硬件安全完整性的必要步骤的概述,以及该条款与 GB/T 20438 的其他要求的关系。

对硬件安全完整性而言,可声明的最高的安全完整性等级受限于硬件安全完整性约束,硬件安全完整性约束来自两种可行的路线之一(在系统或子系统级):

——路线 1_H 基于硬件故障裕度和安全失效分数的概念;

——路线 2_H 基于由最终用户反馈的元器件可靠性数据、对指定的安全完整性等级增强的置信度和硬件故障裕度。

基于 GB/T 20438 的应用标准可能会给出优先路线(即路线 1_H 或路线 2_H)。

注 3:上述路线的下标“H”指硬件安全完整性,以便与系统安全完整性的路线 1_S、2_S 与 3_S 进行区分。

7.4.4.1 一般要求

7.4.4.1.1 关于硬件故障裕度的要求

a) 硬件故障裕度 N 意味着 N+1 个故障会导致安全功能的丧失(更详细参见注 1、表 2 和表 3)。

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) 如果一个故障直接引起一个或多个后续故障，这些故障都视为是单个故障；

c) 确定实现的硬件故障裕度时，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。应证明不考虑这类故障的合理性并建立文档(见注 2)。

注 1：为了获得足够健壮的架构，需要将硬件安全完整性的约束条件考虑在内，组件和子系统的复杂程度也要包括在内(见 7.4.4.1.1 和 7.4.4.1.2)。根据这些要求，E/E/PE 安全相关系统执行的安全功能的最高允许安全完整性等级，为该安全功能所允许的最大值，即便有些情况下可靠性计算表明可以达到更高的安全完整性。同时需要注意的是，即使所有子系统的硬件故障裕度都已经实现，还是有必要通过可靠性计算证明达到了规定的目标失效量，这可能需要提高硬件故障裕度以满足设计要求。

注 2：该硬件故障裕度要求适于在正常工作条件下使用的子系统架构。在线维修 E/E/PE 安全相关系统时，可适当放宽硬件故障裕度要求，但宜事先评估放宽硬件故障裕度相关的关键参数(如 MTTR 与提出要求的概率作比较)。

注 3：某些特定故障可予排除，因为如果某个组件因设计与结构的固有属性而具有极低的失效概率(如机械执行器连接件)，则通常无需考虑因使用该组件而对安全功能安全完整性造成的约束(基于硬件故障裕度)。

注 4：路线的选择取决于应用与领域，同时宜考虑以下因素：

——某个功能的安全失效可能会引发新的危险，或成为某个已存在危险的额外诱因；

——冗余可能并不适用于所有的功能；

——维修并不总是可行的或快速的(如所需时间与检验测试间隔相比无法忽略)。

注 5：在附录 E 中给出了集成电路片上冗余的特殊架构要求。

7.4.4.1.2 如果要实现安全功能的元器件满足下列全部条件，则组件可视为 A 类：

a) 所有组成元器件的失效模式都被明确定义；

b) 故障状况下组件的行为能够完全确定；

c) 有充足而可靠的失效数据，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 7.4.9.3～7.4.9.5)。

7.4.4.1.3 如果要实现安全功能的元器件满足下列条件之一，则组件应视为 B 类：

a) 至少一个组成元器件的失效模式未被明确定义；

b) 故障状况下组件的行为不能完全确定；

c) 没有充足而可靠的失效数据，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 7.4.9.3～7.4.9.5)。

注：这就是说，如果组件中只要有一个组成元器件满足 B 类的条件，那么这个组件将被视为 B 类，而不是 A 类。

7.4.4.1.4 估算组件的安全失效分数时，如组件用于硬件故障裕度为 0 的子系统，且该子系统安全功能或部分安全功能需要在高要求或连续运行模式下运行，则仅在满足以下任一条件时诊断可予以采信：

——诊断测试间隔和执行特定功能以获得或维持安全状态的时间总和小于过程安全时间；

——当工作在高要求运行模式下，诊断测试率与要求率之比等于或大于 100。

7.4.4.1.5 当估算以下组件的安全失效分数时，

——硬件故障裕度大于 0，且安全功能或部分安全功能需要在高要求或连续运行模式下运行；

——安全功能或部分安全功能需要在低要求运行模式下运行。

如果诊断测试间隔和对检测到的故障的维修时间的总和小于在计算特定安全功能安全完整性时所用的 MTTR，诊断可予以采信。

7.4.4.2 路线 1_H

7.4.4.2.1 为了确定规定的安全功能所声明的最高安全完整性等级，应遵循以下步骤：

1) 定义构成 E/E/PE 安全相关系统的子系统。

2) 确定每个子系统中所有组件各自的安全失效分数(即逐个组件进行，每个组件的硬件故障裕度为 0)。对于冗余组件配置，计算 SFF 时可考虑可用的额外诊断(如通过冗余组件的比较)。

3) 对于每个组件,通过所达到的安全失效分数与硬件故障裕度0来确定声明的最高安全完整性等级,见表2第2栏(A类组件)与表3第2栏(B类组件)。
4) 使用7.4.4.2.3和7.4.4.2.4的方法确定子系统声明的最高安全完整性等级。
5) E/E/PE安全相关系统声明的最高安全完整性等级应由子系统中最低安全完整性等级所决定。

7.4.4.2.2 对于子系统由满足规定要求(以下详述)的组件构成的应用,作为采用7.4.4.2.1 2)~7.4.4.2.1 4)的要求的替代,以下(要求)适用:

1) 子系统由一个以上的组件组成;且
2) 组件类型相同;且
3) 所有组件达到了表2或表3中规定的在相同的范围区间内的安全失效分数,那么按照如下的步骤:
   a) 确定所有独立组件的安全失效分数。对于冗余组件配置,计算SFF时应考虑可用的额外诊断(如通过比较冗余组件);
   b) 确定子系统的硬件故障裕度;
   c) 如果是A类组件,按照表2确定子系统可声明的最高安全完整性等级;
   d) 如果是B类组件,按照表3确定子系统可声明的最高安全完整性等级。

注1:上文3)中的范围对应于表2与表3中安全失效分数为四个中的一个[即<60%;60%至<90%;90%至<99%;≥99%)时的值。所有SFF都需处于同一范围(如均在90%至99%)]。

示例1:对于硬件故障裕度为1且组件安全功能通过并联组件实现的子系统,如果子系统满足7.4.4.2.2中要求,可使用以下方法确定规定的安全功能达到的最大允许安全完整性等级。此例中,所有组件为B类,而组件的安全失效分数在90%至<99%范围。

由表3可看出,如硬件故障裕度等于1而两个组件的安全失效分数在90%至<99%范围内,则安全功能的最大允许安全完整性等级为SIL 3。

示例2:对于组件安全功能通过并联组件实现的子系统,如果子系统满足7.4.4.2.2中要求,可使用以下方法确定子系统中规定的安全功能的所需硬件故障裕度。此例中,所有组件为A类,而组件的安全失效分数在60%至<90%范围。则规定的安全功能的最大允许安全完整性等级为SIL 3。

由表2可见,为满足SIL 3要求,所需硬件故障裕度需为1,即需要并联两个组件。

表2 A类安全相关组件或子系统执行安全功能时的最大允许安全完整性等级

组件的安全失效分数	硬件故障裕度		
	0	1	2
<60%	SIL 1	SIL 2	SIL 3
60%~<90%	SIL 2	SIL 3	SIL 4
90%~<99%	SIL 3	SIL 4	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

注1:本表对应于7.4.4.2.1与7.4.4.2.2,在给定子系统故障裕度与所用组件SFF的情况下,确定某个子系统可达到的最高SIL。
1) 子系统一般应用参见7.4.4.2.1。
2) 对于包含符合7.4.4.2.2要求的组件的子系统,如果要直接通过本表声明子系统满足规定的SIL,则需满足7.4.4.2.2中所有的要求。

注2:对于7.4.4.2.1与7.4.4.2.2,本表也可用于:
1) 如果给定子系统安全功能所要求的SIL和使用组件的SFF,可确定硬件故障裕度。
2) 如果给定子系统安全功能所要求的SIL和子系统的硬件故障裕度,可确定组件SFF的要求。

注3:7.4.4.2.3与7.4.4.2.4中的要求是基于本表及表3中给出的数据。

注4:附录C给出了如何计算安全失效分数的具体方法。

表 3　B 类安全相关组件或子系统执行安全功能时的最大允许安全完整性等级

组件的安全失效分数	硬件故障裕度		
	0	1	2
＜60％	不允许	SIL 1	SIL 2
60％～＜90％	SIL 1	SIL 2	SIL 3
90％～＜99％	SIL 2	SIL 3	SIL 4
≥99％	SIL 3	SIL 4	SIL 4

注 1：本表对应于 7.4.4.2.1 与 7.4.4.2.2，在给定子系统故障裕度与所用组件 SFF 的情况下，确定某个子系统可达到的最高 SIL。

1）　子系统一般应用参见 7.4.4.2.1。

2）　对于包含符合 7.4.4.2.2 要求的组件的子系统，如果要直接通过本表声明子系统满足规定的 SIL，则需满足 7.4.4.2.2 中所有的要求。

注 2：对于 7.4.4.2.1 与 7.4.4.2.2，本表也可用于：

1）　如果给定子系统安全功能所要求的 SIL 和使用组件的 SFF，可确定硬件故障裕度。

2）　如果给定子系统安全功能所要求的 SIL 和子系统的硬件故障裕度，可确定组件 SFF 的要求。

注 3：7.4.4.2.3 与 7.4.4.2.4 中的要求是基于本表及表 2 中给出的数据。

注 4：附录 C 给出了如何计算安全失效分数的具体方法。

注 5：使用 7.4.4.2.1 中方法组合硬件故障裕度为 1 的 B 类组件时，如果所组合的两个组件的安全失效分数都小于 60％，则组合成的安全功能的最大允许安全完整性等级为 SIL 1。

7.4.4.2.3　在一个 E/E/PE 安全相关子系统中通过组件串联（如图 5 所示）实现多个组件安全功能时，此类组合安全功能可声明的最高安全完整性等级，取决于硬件故障裕度为 0 时安全失效分数最低的那个组件。为阐释这一方法，可假定某个架构如图 5 所示。

示例：（见图 5）：假定某架构中的数个组件安全功能通过子系统执行，而该子系统又包含由组件 1、2 与 3 组成的单通道，且组件均满足表 2 与 3 中的如下要求：

——组件 1：硬件故障裕度为 0，给定安全失效分数，满足 SIL1 的要求；

——组件 2：硬件故障裕度为 0，给定安全失效分数，满足 SIL2 的要求；

——组件 3：硬件故障裕度为 0，给定安全失效分数，满足 SIL1 的要求；

——可声明的最高 SIL 等级受限于组件 1 及组件 3，可达到的硬件故障裕度与安全失效分数仅为 SIL 1。

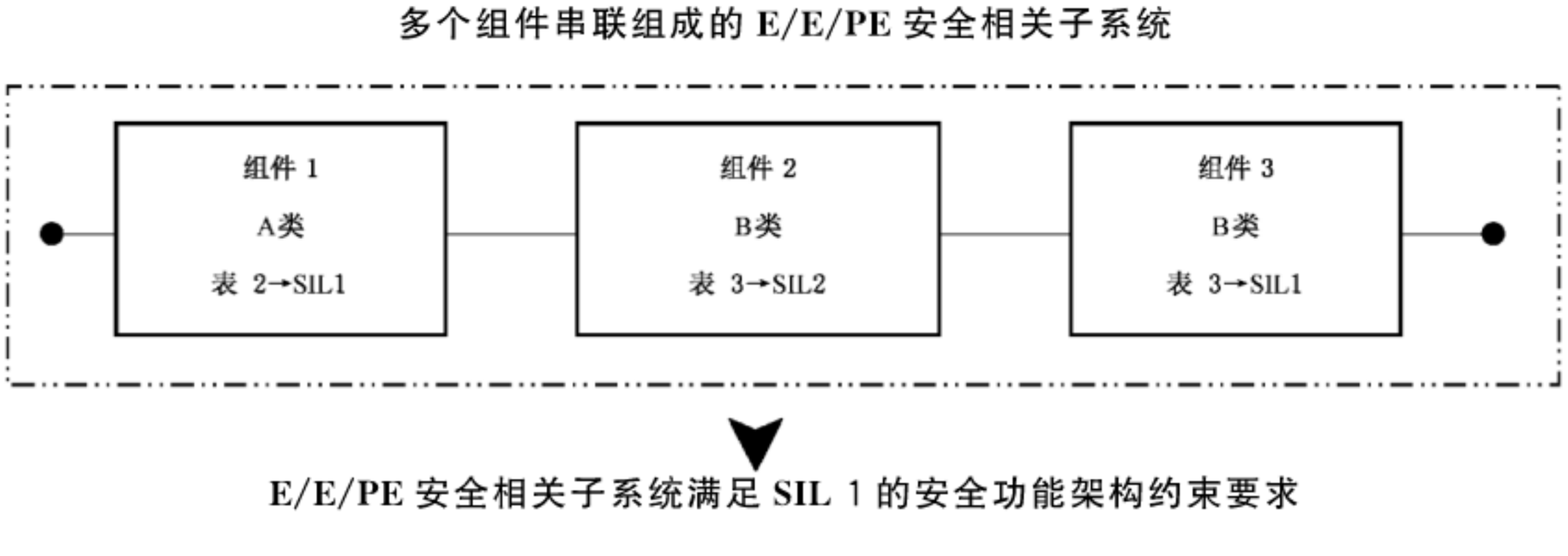


图 5　确定规定架构的最高 SIL（包含数个串联组件的 E/E/PE 安全相关子系统，见 7.4.4.2.3）

7.4.4.2.4　一个 E/E/PE 安全相关子系统，其组件的安全功能是由几条通道（组件并联组合）来实现，且硬件故障裕度为 N，其安全功能所声明的最高安全完整性等级应由如下决定：

a）　将每条通道中串联组合的组件分组，并确定这些通道中安全功能所能宣称的最高的安全完整性等级（见 7.4.4.2.3）；并且

b）　选择完成安全功能中获得最高安全完整性的通道，然后安全完整性等级加 N，以决定子系统整体组合后的最高安全完整性等级。

为了说明该方法，假设图 6 中给出的架构并见如下示例。

注 1：N 是并联组件组合后的硬件故障裕度（见 7.4.4.1.1）。

注 2：关于本条的应用见如下示例。

示例：这些组合的分组与分析方法有多种。在此说明其中一种方法，假定架构中安全功能通过两个子系统 X 与 Y 实现，其中子系统 X 由组件 1、2、3 与 4 组成，子系统 Y 由单个组件 5 组成，如图 6 所示。子系统 X 中使用并联通道确保组件 1 与 2 可独立实现子系统 X 所需的部分安全功能，而与组件 3 与 4 无关，反之亦然。该安全功能在以下情况下仍有效：

——组件 1 或 2 出现故障（因为组件 3 和 4 的组合能够实现所需要的安全功能）；或

——组件 3 或 4 出现故障（因为组件 1 和 2 的组合能够实现所需要的安全功能）。

确定相关安全功能可声明的最高安全完整性等级的详细步骤如下。

对于子系统 X 的特定安全功能，每个组件满足表 2 与 3 中的如下要求：

——组件 1：硬件故障裕度为 0，给定安全失效分数，安全完整性等级为 SIL3；

——组件 2：硬件故障裕度为 0，给定安全失效分数，安全完整性等级为 SIL2；

——组件 3：硬件故障裕度为 0，给定安全失效分数，安全完整性等级为 SIL2；

——组件 4：硬件故障裕度为 0，给定安全失效分数，安全完整性等级为 SIL1；

以下组件组合方式可为子系统 X 中的相关安全功能提供最高的硬件安全完整性等级：

a）　组合组件 1 与 2：组件 1 与 2 的组合可达到的硬件故障裕度与安全失效分数（每个组件分别满足 SIL 3 与 SIL 2 的要求）满足 SIL 2 的要求（由组件 2 决定，见 7.4.4.2.3）；

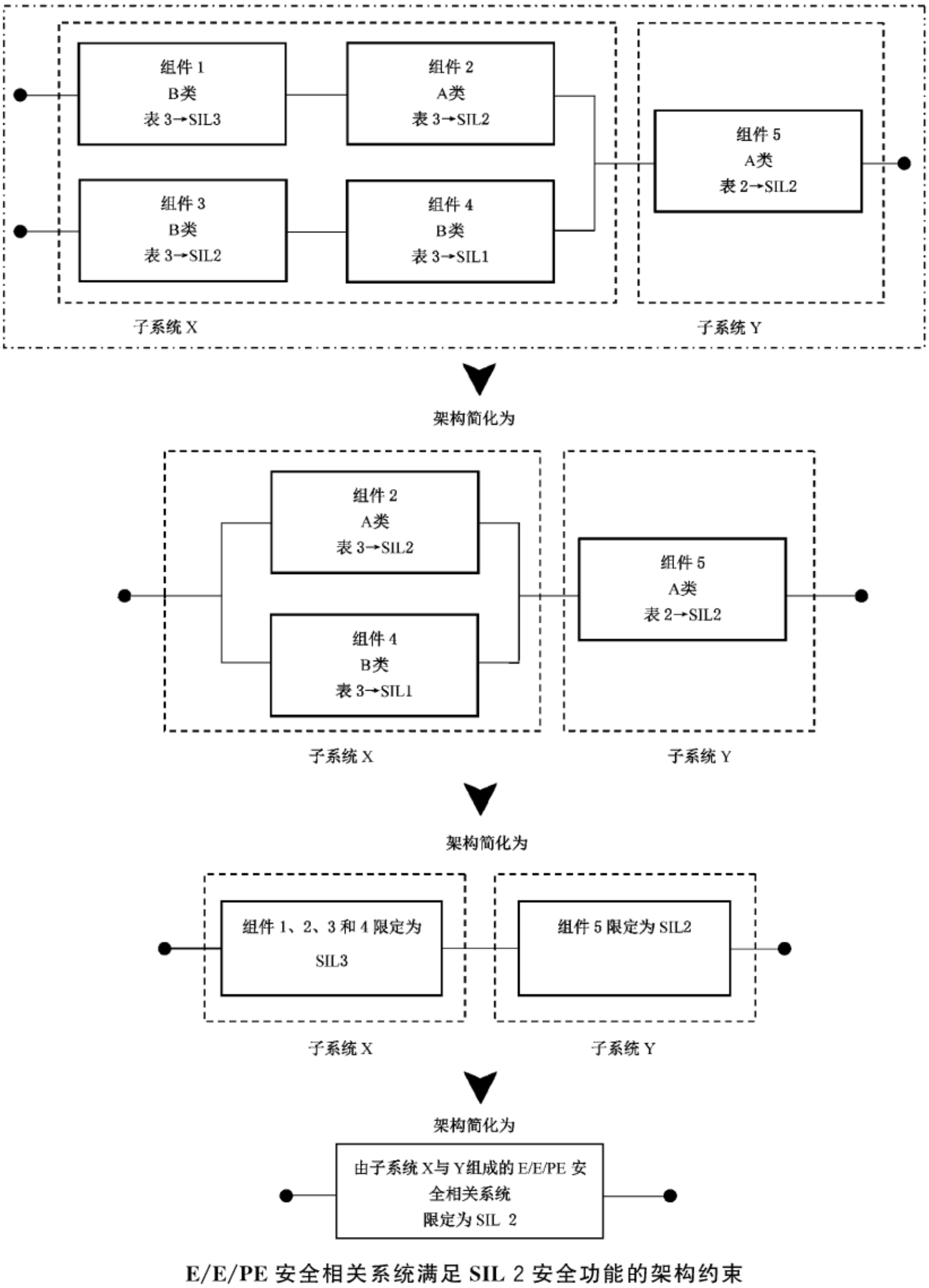
b）　组合组件 3 与 4：组件 3 与 4 的组合可达到的硬件故障裕度与安全失效分数（每个组件分别满足 SIL 2 与 SIL 1 的要求）满足 SIL 1 的要求（由组件 4 决定，见 7.4.4.2.3）；

c）　组件 1、2 组合体与组件 3、4 组合体的进一步组合：确定相关安全功能可达到的最高安全完整性等级时，可选择达到的安全完整性等级最高的通道并加上 N 个安全完整性等级，得到整个组件组合的最高安全完整性等级。此例中子系统包含两个并联通道，其硬件故障裕度为 1，相关安全功能安全完整性等级最高的通道由组件 1 与 2 的组成，达到 SIL 2 的要求。因此，硬件故障裕度为 1 时该子系统的最高安全完整性等级为（SIL 2＋1）＝SIL 3（见 7.4.4.2.4）。

对于子系统 Y，组件 5：故障裕度为 0，给定安全失效分数，安全完整性等级为 SIL2。

对于一个完整的 E/E/PE 安全相关系统（包含两个子系统 X 与 Y，相关安全功能分别满足 SIL 3 与 SIL 2），其可达到的最高安全完整性等级由安全完整性等级最低的子系统决定（7.4.4.2.1 5）。因此，此例中 E/E/PE 安全相关系统中相关安全功能的最高安全完整性等级为 SIL 2。

由两个子系统 X 与 Y 组成的 E/E/PE 安全相关系统



E/E/PE 安全相关系统满足 SIL 2 安全功能的架构约束

注 1：组件 1 与 2 可独立实现子系统 X 所需的部分安全功能，而与组件 3 与 4 无关，反之亦然。

注 2：实现该安全功能的子系统在范围上覆盖了从传感器到执行器的整个 E/E/PE 安全相关系统。

图 6　确定规定架构的最高 SIL(由两个子系统 X 与 Y 组成的 E/E/PE 安全相关子系统，见 7.4.4.2.4)

7.4.4.3 路线 2_H

7.4.4.3.1 对于实现规定安全完整性等级的安全功能的 E/E/PE 安全相关系统，其每个子系统的最小硬件故障裕度如下：

注：在以下条款中，除非另行规定，安全功能既可在低要求模式下运行，也可在高要求或连续运行模式下运行。

a) 除非适用 7.4.4.3.2 的条件，对于规定达到 SIL4 的安全功能，硬件故障裕度为 2。

b) 除非适用 7.4.4.3.2 的条件，对于规定达到 SIL3 的安全功能，硬件故障裕度为 1。

c) 除非适用 7.4.4.3.2 的条件，对于规定达到 SIL2 的安全功能，工作在高要求或连续运行模式下，硬件故障裕度为 1。

d) 对于规定达到 SIL 2 的安全功能，工作在低要求运行模式下，硬件故障裕度为 0。

e) 规定达到 SIL 1 的安全功能，硬件故障裕度为 0。

7.4.4.3.2 仅对 A 类组件，如果 HFT 按照 7.4.4.3.1 中规定的要求来确定，假设要求 HFT 大于 0，将会引入额外的失效并导致 EUC 整体安全性降低，则可以采用降低 HFT 的更安全的替代架构来实现。这种情况下应做评估并建立文档。评估应提供如下证据：

a) 遵循 7.4.4.3.1 中规定的 HFT 的要求会引入额外的失效并导致 EUC 整体安全的降低；并且

b) 如果 HFT 降低为 0，在组件执行安全功能时辨识出的失效模式可以被排除，因为辨识出的失效模式的危险失效率相比于安全功能的目标失效量要低[见 7.4.4.1.1 的 c)]。即声明的故障排除的所有串联组件的危险失效频率的总和不应超过目标失效量的 1%。此外，在评价故障排除的适应性时应考虑系统性故障的潜在可能。

注：故障裕度是构建一个健壮架构实现的所要求置信度的优选方法。当满足 7.4.4.3.2 中条件时，论证的目的是证明所提出的替代架构与原方案相当甚至更优。这可能取决于技术领域和/或应用。例如：备份安排(如分析冗余、通过其他传感器输出的物理计算结果代替故障传感器输出)；同一技术中尽量使用最可靠的组件(如果可行)；更换为更可靠的技术；使用多样化技术减少共因失效的影响；增加设计裕度；限制环境条件(如电子元器件)；通过收集大量现场反馈或专家判断降低可靠性的不确定度。

7.4.4.3.3 如果选择路线 2_H，那么当使用可靠性数据来量化随机硬件失效的影响时(见 7.4.5)，应该：

a) 基于在役组件在类似应用和环境下的现场反馈；和

b) 基于按照国际标准(例如，IEC 60300-3-2 或 ISO 14244)采集的数据；和

c) 依据以下条款的评价：

1) 大量的现场反馈；和

2) 专家判断；和

3) 如有必要，实施特定的测试。

以预估计算中所用各个可靠性参数(如失效率)的平均值与不确定度(如 90%置信区间或概率分布见注 2)。

注 1：鼓励最终用户按照已发布标准组织相关元器件可靠性数据的收集。

注 2：失效率 λ 的 90%置信区间是指，其实际值有 90%的概率落在这一区间$[\lambda_{5\%}, \lambda_{95\%}]$。$\lambda$ 有 5%的概率优于 $\lambda_{5\%}$ 而差于 $\lambda_{95\%}$。基于纯粹的统计学，平均失效率可使用“最大似然估算法”预估，置信区间$(\lambda_{5\%}, \lambda_{95\%})$可使用 χ^2 函数计算。精确度取决于累计的观测时间与所观察到的失效次数。可使用贝叶斯方法处理统计观察、专家判断与具体试验结果。可由此拟合相关的概率分布函数，用于后续的蒙特卡罗仿真。

如选择了路线 2_H，则计算目标失效量时(即 PFD_{avg} 或 PFH)应考虑可靠性数据不确定度，并应改进系统直至目标失效量达到 90%以上的置信度。

7.4.4.3.4 路线 2_H 中使用的所有 B 类组件的最小诊断覆盖率不应低于 60%。

7.4.5 量化随机硬件失效影响的要求

注：GB/T 20438.6—2017 中附录 A.2 给出了达到要求的硬件安全完整性必要步骤的概述，并说明了本条款和 GB/T 20438 其他要求之间的关系。

7.4.5.1 对于每个安全功能，在随机硬件失效（包括软错误）与数据通信过程随机失效影响下 E/E/PE 安全相关系统可达到的安全完整性应按照 7.4.5.2 与 7.4.11 估算，且结果应小于等于 E/E/PE 系统安全要求规范中规定的目标失效量（见 GB/T 20438.1—2017 的 7.10）。

注：为证明已达到要求，应使用适当技术（见 7.4.5.2）进行相关功能的可靠性预测，并与相关安全功能的目标失效量进行比较（见 GB/T 20438.1）。

7.4.5.2 对 7.4.5.1 中每个安全功能达到的失效量的估算应考虑以下因素：

a) E/E/PE 安全相关系统及其子系统架构以及与相关安全功能的关系；

注 1：这里需要确定系统的组件在哪种失效模式下为串联配置（即任何失效都会导致所执行的相关安全功能的失效），以及在哪种失效模式下为并联配置（即多个失效同时发生时相关安全功能才会失效）。

b) E/E/PE 安全相关系统的各子系统的组件架构，以及与所考虑的各个安全功能的关系；

c) 估算在任何模式下可能导致 E/E/PE 安全相关系统发生危险失效但会被诊断测试（见 7.4.9.4～7.4.9.5）检测到的各子系统及其组件的失效率，应根据数据源及其精度或裕度对失效率进行论证。这可能包括考虑和比较不同来源的数据，并且选择和所考虑的系统组合最相近的失效率。量化随机硬件失效影响与计算安全失效分数或诊断覆盖率所用的失效率应考虑规定的运行条件；

注 2：考虑运行条件意味着通常需调整来自数据库的失效率，如触点负载和温度的影响。

d) E/E/PE 安全相关系统及其子系统对于共因失效（见注 3 与注 4）的敏感性。应对假设进行论证；

注 3：共因失效可能是由硬件组件实际失效之外的因素导致（如电磁干扰与解码错误等）。但 GB/T 20438 中计算随机硬件失效的影响时需考虑此类失效。组件交叉测试可降低共因失效的可能性。

注 4：如 E/E/PE 安全相关系统与要求原因或其他保护层之间存在共因失效，则需证实在确定安全完整性等级与目标失效量要求时已考虑此因素。确定共因因子的方法见 GB/T 20438.6—2017 的附录 D。

e) 各子系统的诊断测试的诊断覆盖率（按附录 C 确定），相关的诊断测试间隔，以及由于随机硬件失效导致的危险未揭露的失效率。当相关时，只有满足 7.4.5.3 中要求的诊断测试才予以考虑。可靠性模型中应考虑 MTTR 与 MRT（见 GB/T 20438.4—2017 中 3.6.21 与 3.6.22 部分）；

注 5：确定诊断测试间隔时，需考虑与诊断覆盖率相关的所有测试时间间隔。

f) 用于揭露危险故障的检验测试间隔；

g) 检验测试是否为 100%有效；

注 6：不完善的检验测试会使安全功能无法恢复至“如同新的一样好”的状态，因此失效概率相应增加。宜对各项假设进行论证，尤其宜包括组件的可更新周期或对安全功能在整个生命周期内风险降低的影响。进行测试时如为离线测试，应考虑测试持续时间。

h) 检测出失效后的维修时间；

注 7：平均维修时间（MRT）是平均恢复时间（MTTR）中的一部分（见 GB/T 20438.4—2017 中 3.6.22 与 3.6.21），MTTR 还包括检测失效所用时间以及无法进行维修的时间（见 GB/T 20438.6—2017 的附录 B，如何使用 MTTR 与 MRT 计算失效概率）。仅在 EUC 关闭或在安全状态下维修时才可认为是即时维修。如无法在 EUC 停车及在安全状态下进行维修，尤其需全面考虑无法进行维修的时间，特别是该时间段相对较长时。与维修相关的所有因素均宜考虑。

i) 如需人员操作来实现安全功能，则应考虑随机人为错误的影响；

注 8：如人员接到不安全情况报警并需采取措施，则宜考虑人为错误的随机性，且整个计算中宜包括人为错误的可能性。

j) 事实上有多种建模方法，最适合的方法需由分析人员确定并取决于具体情况。可行方法包括因果分析(GB/T 20438.7—2017 中 B.6.6.2)、故障树分析(GB/T 20438.7—2017 中 B.6.6.5)、马尔可夫模型(GB/T 20438.6—2017 中附录 B 与 GB/T 20438.7—2017 中 B.6.6.6)、可靠性框图(GB/T 20438.6—2017 中附录 B 与 GB/T 20438.7—2017 中 B.6.6.7)以及佩特里网(GB/T 20438.6—2017 中附录 B 与 GB/T 20438.7—2017 中 B.2.3.3)。

注 9：GB/T 20438.6 的附录 B 中给出了一种简单方法，可用于估算由于随机硬件失效导致的对安全功能要求时的危险失效平均概率，以确定架构满足要求的目标失效量。

注 10：GB/T 20438.6—2017 中 A.2 给出了实现所需硬件安全完整性的必要步骤，以及该条款与 GB/T 20438 的其他要求的关系。

注 11：对于每个安全功能需要单独计算 E/E/PE 安全相关系统的可靠性，因为组件失效模式不同，E/E/PE 安全相关系统的架构(就冗余而言)也可能不同。

7.4.5.3 量化子系统的随机硬件失效影响时，如组件用于硬件故障裕度为 0 的子系统，且该子系统安全功能或部分安全功能需要在高要求或连续运行模式下运行，则仅在满足以下任一条件时诊断可予以采信：

——诊断测试间隔和执行特定功能以获得或维持安全状态的时间总和小于过程安全时间；

——当工作在高要求运行模式下，诊断测试率与要求率之比等于或大于 100。

7.4.5.4 任何子系统的诊断测试间隔：

——硬件故障裕度大于 0，并在高要求或连续运行模式下运行安全功能或部分安全功能；或

——在低要求运行模式下运行安全功能或部分安全功能。

应确保诊断测试间隔与维修检测出失效所用时间的总和小于计算确定该安全功能的安全完整性所用的 MTTR。

7.4.5.5 如果对于某个特定设计，未实现相关安全功能的安全完整性要求，则：

a) 确定对功能失效率贡献最大的组件、子系统和/或参数；

b) 评价可行的改进措施对确定出的关键组件、子系统或参数的影响(如使用更可靠的元器件，附加的共因失效防范措施，提高诊断覆盖率，增加冗余，缩短检验测试间隔，交叉测试等)；

c) 选择并实施可行的改进措施；

d) 重复必要的步骤以确定新的随机硬件失效概率。

7.4.6 避免系统性故障的要求

注：应用此条款要求时，详情参见 7.4.2.2c)。

7.4.6.1 设计和开发 E/E/PE 安全相关系统的软硬件时，为避免引入故障，应采用一组适当的技术措施(参见表 B.2 和 GB/T 20438.3)。

注：GB/T 20438 不包括在设计大批量生产的电子集成电路(如标准化微处理器)时，避免系统性故障相关的特定要求。这是因为通过严谨的开发规程、严酷的测试以及利用用户反馈意见获取的丰富经验，此类设备发生故障的可能性已降至最低。对于无法满足此基础(如新设备或 ASIC)的电子集成电路，如果要将其应用于 E/E/PE 安全相关系统，可采用对 ASIC 的要求(参见 7.4.6.7 及资料性附录 F)。在有疑问(关于利用用户反馈意见获取的丰富经验)的情况下，表 B.6 中对“现场经验”的要求还宜考虑到 SIL 1 和 SIL 2“低”的有效性，SIL 3“中”和 SIL 4“高”的有效性。

7.4.6.2 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；
——子系统和组件接口；
——顺序和时间相关信息；
——并发性和同步化。
c) 清晰、准确的文档和信息的交流；
d) 验证和确认。

7.4.6.3 为保证 E/E/PE 安全相关系统的安全完整性要求能持续得到满足，在设计阶段就应将维护要求规范化。

7.4.6.4 如适用，应使用自动测试工具和集成开发工具。

7.4.6.5 设计期间，应编制 E/E/PE 系统的集成测试计划。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) 通过/不通过的准则。

7.4.6.6 设计期间，可在开发者工作场所执行的活动，应与需在用户现场执行的活动加以区分。

7.4.6.7 为避免在设计开发 ASIC 的过程中引入故障，应该采用一组必要的、适当技术和措施。

注：资料性附录 F 中给出了支持相关特性实现的技术和措施。图 3 所示为相关 ASIC 的开发生命周期。

7.4.7 控制系统性故障的要求

注：使用本条款要求时，详情参见 7.4.2.2 c)。

7.4.7.1 为控制系统性故障，E/E/PE 系统的设计特点应使得 E/E/PE 安全相关系统能容许：
a) 硬件中的任何残余设计故障，除非能排除硬件设计故障的可能性(见表 A.15)；
b) 环境应力，包括电磁干扰(见表 A.16)；
c) EUC 操作员造成的失误(见表 A.17)；
d) 软件中的任何残余设计故障(见 GB/T 20438.3—2017 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 7.4.11)。

7.4.7.2 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。

7.4.7.3 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，并应合理分配操作者和维护人员的活动。所有接口的设计应更好的依据人员操作习惯并应适合操作者的认知能力和培训水平，例如操作者为普通人员的大批量生产的 E/E/PE 安全相关系统。

注 1：设计目标宜是，对操作者和维护人员所犯的可预见的致命错误，只要有可能都可通过设计来防止或消除，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错误也许不能被 E/E/PE 安全相关系统所弥补，例如，在 EUC 内部的一些机械失效，除非通过直接检查，否则不能被检测到或不能被实际弥补。

7.4.8 检测到故障时的系统行为要求

注：本部分的要求适用于由单一 E/E/PE 安全相关系统所执行的规定的安全功能，且整体安全功能未分配给其他风险降低措施。

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

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,以保证 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 7.4.5.2)时设定的平均维修时间(MRT)(见 GB/T 20438.4—2017 中的3.6.22)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/PE 系统安全要求中给出为达到或保持安全状态所要求的动作(见 GB/T 20438.1—2017 的 7.10)。它可能包括,例如,安全关闭 EUC,或者为了功能安全,安全关闭与故障子系统相关的 EUC 部分。

7.4.8.2 对于硬件故障裕度等于零的情况,当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 7.4.5.2)时设定的平均维修时间(MRT)(见 GB/T 20438.4—2017 中 3.6.22)内,维修故障子系统。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安全完整性至少应等于无任何故障的 E/E/PE 系统安全相关系统提供的安全完整性。应在 E/E/PE 系统运行和维护规程中对附加措施和约束进行规定(见 7.6)。

注:在 E/E/PE 系统安全要求规范中给出为达到或保持安全状态所要求的动作(见 GB/T 20438.1—2017 的7.10)。它可能包括,例如,安全关闭 EUC,或者为了功能安全,安全关闭与故障子系统相关的 EUC 部分。

7.4.8.3 对于硬件故障裕度等于零的子系统,当该子系统在高要求或连续运行模式下运行安全功能时,检测出的危险故障(通过诊断测试,检验测试或其他方法)应采取规定的动作以达到或维持安全状态(见注)。

注:在 E/E/PE 系统安全要求中给出为达到或保持安全状态所要求的动作(见 GB/T 20438.1—2017 的 7.10)。它可能包括,例如,安全关闭 EUC,或者为了功能安全,安全关闭与故障子系统相关的 EUC 部分。

7.4.9 E/E/PE 系统实现的要求

7.4.9.1 应根据 E/E/PE 系统的设计要求规范来实现 E/E/PE 安全相关系统(见 7.2.3)。

7.4.9.2 被一个或多个安全功能使用的所有子系统及其组件都应作为安全相关子系统或组件进行标识并建立文档。

7.4.9.3 应针对每个安全相关子系统和组件提供以下信息(亦可参见 7.4.9.4):

注:声明符合 GB/T 20438 的安全相关子系统或组件供应商有必要在符合项安全手册(参见附录 D)中为安全相关系统(或其他子系统或组件)的设计者提供这些信息。

a) 子系统及其相应组件的功能规范;

b) 与子系统及其组件的应用相关的所有说明或限制,这些内容应该严格遵守,以避免出现子系统的系统性失效;

c) 每个组件的系统性能力[参见 7.4.2.2 的 c)];

d) 对组件的硬件和/或软件配置进行标识以使配置管理符合 GB/T 20438.1—2017 的 6.2.1;

e) 验证子系统及其组件已满足 E/E/PE 设计要求规范(参见 7.2.3)中的功能要求和系统性能力的相关文档证据。

7.4.9.4 应针对每个可能发生随机硬件失效(另请参见 7.4.9.3 和 7.4.9.5)的安全相关组件提供以下信息:

注 1:声明符合 GB/T 20438 的组件供应商有必要在组件安全手册(参见附录 D)中为安全相关系统的设计者提供这些信息。

a) 导致安全功能失效的组件失效模式(就其输出行为来说),这些失效源于组件内部诊断测试未检测到的或者组件外部诊断无法检测到的随机硬件失效(参见 7.4.9.5);

b) 在 a)中所述的每种失效模式下,规定的运行条件下的估算失效率;

c) 导致安全功能失效的组件失效模式(就其输出行为来说),这些失效源于组件内部诊断测试检测到的或者组件外部诊断可检测到的随机硬件失效(参见 7.4.9.5);

d) 在 c)中所述的每种失效模式下,规定的运行条件下的估算失效率;

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

f) 为保持由于随机硬件失效引起的估算失效率的有效性,组件的寿命限制;

g) 应保证的定期检验测试和/或维护要求;

h) 对于 c)中由组件内部诊断测试检测到的每一种失效模式,按照附录 C 所导出的诊断覆盖率(参见注 2);

i) 对于 c)中由组件内部诊断测试检测到的每一种失效模式,相应的诊断测试间隔(参见注 2);

注 2:为了声明在 E/E/PE 安全相关系统硬件安全完整性模型的组件中执行的诊断测试操作是可信的,需要提供诊断测试的覆盖率和诊断测试间隔(参见 7.4.5.2、7.4.5.3 和 7.4.5.4)。

j) 由随机硬件失效导致的诊断的失效率;

k) 为导出在诊断检测出故障后的平均维修时间(MRT,参见 GB/T 20438.4—2017 中的3.6.22),所必需的任何附加信息(例如维修时间);

l) 为导出应用在 E/E/PE 安全相关系统中组件的安全失效分数(SFF)所必需的所有信息,安全失效分数按照附录 C 进行确定,包括根据 7.4.4 分类为 A 类或 B 类;

m) 组件的硬件故障裕度。

7.4.9.5 由于随机硬件失效造成的组件失效的估算失效率[见 7.4.9.4 的 a)和 c)],可通过以下方式之一确定:

a) 利用行业公认的组件失效数据,通过对设计做失效模式和影响分析来确定;

b) 基于组件在以往类似环境条件下使用的经验来确定(见 7.4.10);

注 1:所使用的所有失效率都宜具有至少 70%的置信度。置信度的统计测定方法请参见参考文献[9]。与其等价的术语"显著性水平"请参见参考文献[10]。

注 2:最好能获得现场特定的的失效数据,否则,只能采用通用数据。

注 3:大多数概率估算方法假定失效率为一恒量,但前提条件是组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组件使用寿命的规范。使用寿命高度依赖于组件本身和工作条件,特别是温度(例如,电解电容可能是非常敏感的)。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组件,其寿命将可能大大降低。

7.4.9.6 供应商应根据附录 D 的要求,为符合项提供一份安全手册,手册内容应包括他们所提供的每个符合项及其符合 GB/T 20438 的声明。

7.4.9.7 供应商应该为符合项安全手册中的所有信息提供文档化的证明。

注 1:用充足的证据来支撑所声明的组件安全性能是至关重要的。无支撑的声明无助于建立该组件提供的安全功能的正确性和完整性。

注 2:在证据的可用性方面,可能会有商业或法律上的限制。这些限制超出了 GB/T 20438 的范畴。如果因为这些限制而造成功能安全评估无法充分利用这些证据,那么该组件就不适合用于 E/E/PE 安全相关系统。

7.4.10 经使用证明组件的要求

注:当本部分要求适用时,详见 7.4.2.2c)。

7.4.10.1 对于一个组件来说,只有其具有清晰的、受限的和规定的功能,并且具有充足的文档证据足以说明所有危险的系统性故障发生的可能性足够低,并且可以达到使用该组件的安全功能所需要的安全

完整性等级的情况下，该组件才能被看做是经使用证明的。证据应建立在对特定配置下的组件运行经验进行分析的基础上，同时结合适用性分析和测试。

注：适用性分析和测试侧重于证明组件在预期应用中的性能。已有分析和测试的结果也宜考虑在内。包括功能行为、精度、故障下的行为、时间响应、过载响应、易用性(例如避免人员错误)和可维护性。

7.4.10.2 在7.4.10.1中要求的文档证据应证明：

a) 特定组件之前的使用条件(见注1)与在E/E/PE安全相关系统中将要使用的条件是一致的，或是很接近的；

注1：使用条件(运行环境)包括可能在组件的硬件和软件中引起系统性失效的所有因素。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、编译器和人为因素等。IEC 61784-3中规定了确定运行环境的相似性所需的严格条件。

b) 在以前的使用中没有超出危险失效率。

注2：关于如何使用概率统计方法来确定基于运行经验的已开发软件安全完整性的指南，请参见GB/T 20438.7—2017的附录D。

注3：为经使用证明的组件收集证据需要一个有效的报告失效的系统。

7.4.10.3 当在以前的使用条件和在E/E/PE安全相关系统中所要面对的条件之间存在任何差异时，就应采用适当的分析方法和测试对条件差异进行影响分析，以确定所有危险系统性故障发生的可能性足够低，从而可以让使用该组件的安全功能实现所要求的安全完整性等级。

7.4.10.4 应当使用7.4.10.2所提供的信息建立文档证据，以证明经使用证明的组件能够以所要求的系统性安全完整性为安全功能提供支持。这应该包括以下几个方面：

a) 针对预期应用对组件进行适用性分析和测试；

b) 证明预期运行与先前运行经验的等效性，包括对两者的区别进行影响分析；

c) 统计证据。

7.4.10.5 在确定是否满足上述要求的时候应当考虑以下因素(7.4.10.1～7.4.10.4)，主要有可用信息的覆盖范围和详细程度两个方面(也可见GB/T 20438.1—2017的4.1)：

a) 组件的复杂性；

b) 对组件要求的系统性能力；

c) 设计的新颖性。

7.4.10.6 应该有足够的证据表明，在经使用证明组件的证明材料中未涉及的已有组件功能不应对所使用的组件功能的安全完整性造成不利影响。

注：可以通过以下方式达到该条款的要求：确保以物理或电气方式禁用相应功能；将实现这些功能的软件排除在运行配置之外；或者通过其他形式的论据或证据。

7.4.10.7 对经使用证明组件的所有更改都应满足本部分中7.8和GB/T 20438.3的要求。

7.4.11 数据通信的附加要求

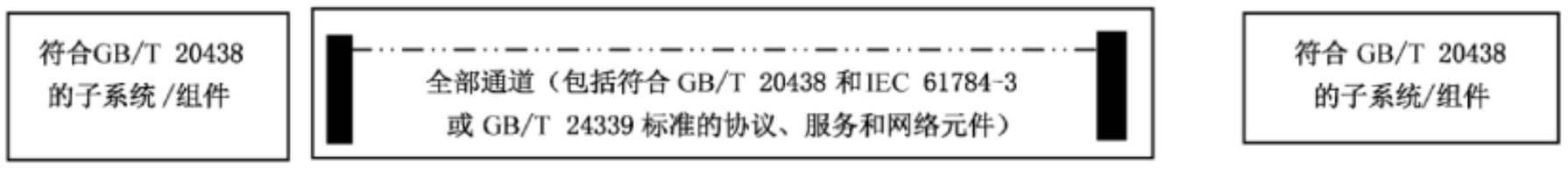
7.4.11.1 当数据通信用于执行一个安全功能时，应估算通信过程中的失效量(例如残余错误率)，包括传输错误、重复、删除、插入、重新排序、误用、延时和伪装。在估算由于随机硬件失效造成的安全功能失效量时应该考虑上述的失效量(参见7.4.5)。

注：术语“伪装”的意思就是没有正确识别出一条信息的真正来源。例如，来自一个非安全组件的信息被错误识别为来自一个安全组件的信息。

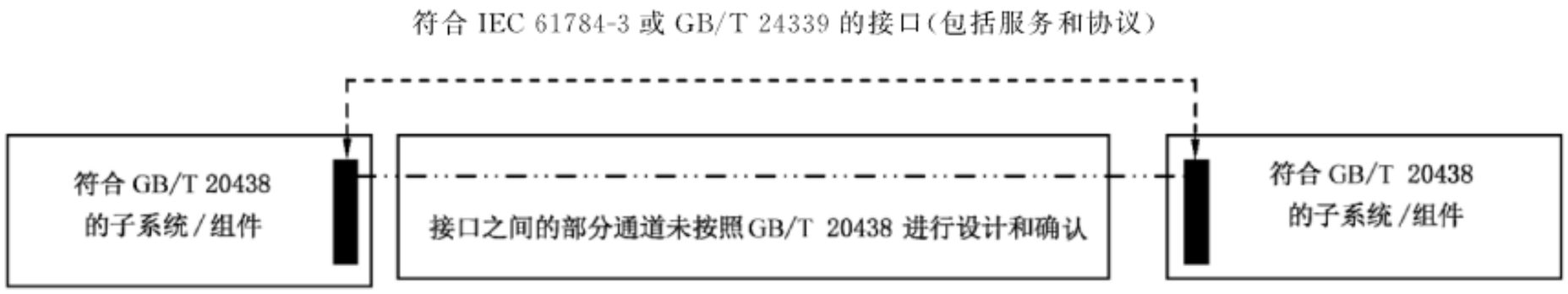
7.4.11.2 为了保证通信过程中要求的失效量(例如残余错误率)，应根据本部分和GB/T 20438.3的要求执行必要的技术和措施。可以通过以下两种方式来实现：

——全部通信通道按照GB/T 20438和IEC 61784-3或IEC 62280的要求进行设计、实现和确认，被称为“白色通道”(参见图7a)；

——部分通信通道未按照 GB/T 20438 的要求进行设计或确认，被称为“黑色通道”（参见图 7b）。在这种情况下，为了保证通信过程的失效性能，应该在 E/E/PE 安全相关子系统或组件中实施必要措施，使这些子系统或组件按照 IEC 61784-3 或 IEC 62280 与通信通道连接。



a） 白色通道



b） 黑色通道

图 7 数据通信架构

7.5 E/E/PE 系统集成

注：这一阶段是图 2 的方框 10.4。

7.5.1 目的

7.5 的目的在于集成和测试 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/PE 系统设计进行集成，并按照规定的 E/E/PE 系统集成测试（见 7.4.2.11）进行测试。

7.5.2.2 作为将所有模块集成到 E/E/PE 安全相关系统的过程的一部分，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（见 GB/T 20438.7—2017 的 B.5.2）进行测试可能就足够了。静态分析（见 GB/T 20438.7—2017 的 B.6.4）、动态分析（见 GB/T 20438.7—2017 的 B.6.5）或者失效分析（参见 GB/T 20438.7—2017 的 B.6.6）可将测试用例减少到一个可接受的程度。如果按照结构化设计（见 GB/T 20438.7—2017 的 B.3.2）或者半形式化方法（见 GB/T 20438.7—2017 的 B.2.3）来进行开发，能够更容易满足要求。

注 2：在使用形式化方法（见 GB/T 20438.7—2017 的 B.2.2）、形式化证明或断言（见 GB/T 20438.7—2017 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—2017 的 B.5.3）。

7.5.2.3 应按照 GB/T 20438.3—2017 的 7.5 的要求将安全相关软件集成到 E/E/PE 安全相关系统中。

7.5.2.4 应生成适当的 E/E/PE 安全相关系统的集成测试文档，给出测试结果，以及说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建立文档。

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，应对所有受影响的组件和子系统进行影响分析并进行必要的重新验证活动。

7.5.2.6 E/E/PE 系统集成测试应对以下信息建立文档：

a) 使用的测试规范的版本；

b) 集成测试的接受准则；

c) 被测试 E/E/PE 安全相关系统的版本；

d) 所使用的工具和设备以及校准数据；

e) 每个测试的结果；

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 为在 E/E/PE 系统集成期间避免故障，应根据表 B.3 采用一组恰当的技术和措施。

7.6 E/E/PE 系统运行和维护规程

注：这一阶段是图 2 的方框 10.5。

7.6.1 目的

7.6 的目的在于制定规程以确保在运行和维护期间保持 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 应准备 E/E/PE 系统运行和维护规程。并应规定如下内容：

a) 为保持“符合设计的”E/E/PE 安全相关系统的功能安全所需执行的例行活动，包括已规定了寿命的组件的例行替换，如冷却风扇、电池等；

b) 为防范非安全状态和/或降低伤害事件造成的后果所必需的活动和约束（例如在安装、启动、正常运行、例行测试、可预见的干扰、故障或失效以及停机期间）；

c) 在系统失效和对 E/E/PE 安全相关系统要求率方面需要维护的文档；

d) 在给出 E/E/PE 安全相关系统的审核和测试结果方面需要维护的文档；

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：

——故障诊断和维修的规程；

——重新确认的规程；

——维护报告要求；

——当原始设备项不可用或被新版本替代时，重新确认的规程。

f) 应制定规程以报告维护的执行，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/PE 系统的运行和维护规程与 EUC 整体的运行和维护规程集成在一起是有益的。

注 2：E/E/PE 系统的运行和维护规程宜包括软件修改规程（见 GB/T 20438.3—2017 的 7.8）。

7.6.2.2 E/E/PE 安全相关系统的运行和维护规程应根据输入，例如：(1)功能安全审核的结果；(2)E/E/PE 安全相关系统的测试，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）所需的例行维护活动应采用系统性的方法来确定。这种方法应可确定所有安全相关组件（从传感器到最终元件）未揭露出的失效，这些失效将导致安全完整性的降低。适用的方法包括：

——故障树检查；

——失效模式和影响分析；

注 1：在确定要求的动作和与 E/E/PE 安全相关系统之间恰当的接口时，人为因素是要考虑的关键因素。

注 2：检验测试的实施将以一定的频率进行，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的维修所需时间依赖于许多因素（见 GB/T 20438.6—2017 的附录 B），包括：

——与安全完整性等级相关的目标失效量；

——架构；

——诊断测试的诊断覆盖率；

——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。实施硬件可靠性分析（见 7.4.5.2）的一个主要原因是保证这两类测试的频率适合于目标硬件安全完整性。

注 5：宜遵照制造商提供的维护要求。对于以可靠性为中心的维护方法，宜经过完整论证（如通过可靠性分析证明其符合 E/E/PE 安全相关系统的目标失效量），才足以采信。

7.6.2.4 应评估 E/E/PE 系统运行和维护规程可能会对 EUC 造成的影响。

7.6.2.5 为在 E/E/PE 系统运行和维护规程中避免故障和失效，应根据表 B.4 采用一组恰当的技术和措施。

7.7 E/E/PE 系统的安全确认

注：这一阶段是图 2 的框 10.6。

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 和 GB/T 20438.1—2017 的 7.10）。

7.7.2 要求

7.7.2.1 E/E/PE 系统安全确认应按照预定计划执行（另见 GB/T 20438.3—2017 的 7.7）。

注 1：在 E/E/PE 系统安全生命周期中显示，E/E/PE 系统安全确认是在安装之前执行的，但在某些情况下，E/E/PE 系统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能完成）。

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 所有确认用的测量设备应依据有据可查的国家标准（如果可能），或依据公认的规程进行校准。所有测试设备应验证能否正确工作。

7.7.2.3 在 E/E/PE 系统安全要求（见 GB/T 20438.1—2017 的 7.10）、E/E/PE 系统设计要求（见 7.2）以及所有 E/E/PE 运行和维护规程中规定的每一个安全功能的有效实现，均应通过测试和/或分析来确认。如果各组件或子系统之间的充分独立或解耦不能被分析证明，应测试相关功能行为的组合。

注：因为必要的测试组合的数量可能很大，在这种情况下可能要求对系统重构。

7.7.2.4 应为所有安全功能制定适用的 E/E/PE 系统安全确认测试的文档，内容包括：

a) 所用的 E/E/PE 系统安全确认计划版本；

b) 待测试（或分析）的安全功能，以及在编制 E/E/PE 系统安全确认计划过程中规定要求的具体参考；

c) 使用的工具和设备，及其校准数据；

d) 每次测试的结果；

e) 预期值和实际结果间的差异。

注：不需要为每一个安全功能建立独立的文档，但每项功能必须包含 a)～e)项中的信息，并且根据不同的安全功能说明其关系。

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/PE 系统安全确认测试的结果建立文档,建立文档内容包括以下信息:

a) 所做的分析;

b) 所做的决策:继续测试或发布修改请求并返回到确认测试的一个早期部分。

7.7.2.6 供应商或开发者应使 EUC 和 EUC 控制系统的开发者能够得到 E/E/PE 系统安全确认测试结果,以使其满足 GB/T 20438.1 中的整体安全确认要求。

7.7.2.7 为在 E/E/PE 系统安全确认过程中避免故障,应根据表 B.5 采用一组适当的技术措施。

7.8 E/E/PE 系统的修改

7.8.1 目的

7.8 要求的目的是在对 E/E/PE 安全相关系统进行改正、增强或适应性修改之后实现并保持所要求的安全完整性

7.8.2 要求

7.8.2.1 应当为每次 E/E/PE 系统的修改活动建立和保持适当的文档记录,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) 变更的进展;

e) 子系统和组件的测试用例,包括重新确认数据;

f) E/E/PE 系统配置管理的历史;

g) 与正常运行和条件的偏差;

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持一种机制,从而在检测到软件和硬件的缺陷时发起变更,并在缺陷影响安全时告知用户有修改的需要。

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—2017 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—2017 的 7.16.2.6。

7.9 E/E/PE 系统的验证

7.9.1 目的

7.9 的目的是测试和评价给定阶段的输出,以保证其对该阶段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,而实际上它们在每个相关阶段中执行。

7.9.2 要求

7.9.2.1 对于 E/E/PE 系统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/PE 系统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/PE 系统验证计划时应规定要执行的具体活动，以保证其对该阶段输入的产品和标准的正确性和一致性。

7.9.2.4 编制 E/E/PE 系统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) 验证活动的选择并建立文档；

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建立文档，内容包括：E/E/PE 安全相关系统已通过验证或未通过原因的说明。应考虑以下因素：

a) 与一个或多个 E/E/PE 系统安全生命周期相关要求不相符的项(见 7.2)；

b) 与一个或多个相关设计标准不相符的项(见 7.4)；

c) 与一个或多个相关安全管理要求不相符的项(见第 6 章)。

7.9.2.7 对于 E/E/PE 系统设计要求的验证，在建立 E/E/PE 系统设计要求(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/PE 系统设计要求规范是否充分满足 E/E/PE 系统安全要求规范(见 GB/T 20438.1—2017 的 7.10)；

b) 检查以下各项间的不兼容性：

——E/E/PE 系统安全要求(见 GB/T 20438.1—2017 的 7.10)；

——E/E/PE 系统设计要求(见 7.2)；

——E/E/PE 系统测试(见 7.4)；

——用户文档和所有其他系统文档。

7.9.2.8 对于 E/E/PE 系统设计和开发验证，在完成 E/E/PE 系统设计和开发(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/PE 系统测试是否适用于 E/E/PE 系统设计和开发；

b) 确定 E/E/PE 系统设计和开发针对 E/E/PE 系统安全要求(见 GB/T 20438.1—2017 的7.10)的一致性和完整性(下至并细化到模块级)；

c) 检查下列各项间的不兼容性：

——E/E/PE 系统安全要求(见 GB/T 20438.1—2017 的 7.10)；

——E/E/PE 系统设计要求(见 7.2)；

——E/E/PE 系统设计和开发(见 7.4)；

——E/E/PE 系统测试(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，将考虑表 A.1 中提供的必须检测的故障和失效。

7.9.2.9 E/E/PE 系统集成验证，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 测试用例和结果应建立文档。

8 功能安全评估

功能安全评估的要求在 GB/T 20438.1—2017 的第 8 章中作了详细说明。

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

A.1 概述

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，本附录推荐了用于控制随机硬件、系统性、环境和操作失效的技术和措施。有关架构和措施的更多信息可参见 GB/T 20438.6—2017 的附录 B 和 GB/T 20438.7—2017 的附录 A。

因为以下两个主要原因，所以无法列出复杂硬件中失效的每个单独的实际起因：

——故障和失效之间的起因/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性失效。

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，包括制造故障和组件选择不正确）；

——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，随机硬件失效，或不正确使用引起的失效）。

为避免和控制这些失效，通常需要大量的措施，附录 A 和附录 B 中的要求把措施分成在 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），以及在运行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.14 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.14 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.15～表 A.17 为每一安全完整性等级推荐了控制系统性失效的技术和措施。表 A.15 为控制系统性失效推荐了整体措施（见 GB/T 20438.3）。表 A.16 为控制环境失效推荐了措施，表 A.17 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.18 进行分级。

GB/T 20438.7—2017 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—2017 的附录 B 给出了确定 E/E/PE 安全相关系统架构的指南。

仅遵从本附录中的指南本身并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；

——针对在每个特定的 E/E/PE 安全相关系统开发过程中所遇到的特殊问题，哪些技术和措施是最适合的。

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应由技术和措施检测出的故障和失效的要求。表 A.2～表 A.14 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.14 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—2017 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.14 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　在量化随机硬件失效的影响时假定的或在推导安全失效分数时要考虑的故障或失效

元器件	见表	所声明的诊断覆盖率要求		
		低(60%)	中(90%)	高(99%)
机电装置	A.2	未加电或断电 触点被熔接	未加电或断电 被熔接的单个触点	未加电或断电 被熔接的单个触点 触点的不正确导向(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) 不正确的打开(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)
分立硬件	A.3，A.7，A.9			
数字 I/O		固定(见注 1)	DC 故障模型(见注 2)	DC 故障模型 漂移和振荡
模拟 I/O		固定	DC 故障模型 漂移和振荡	DC 故障模型 漂移和振荡
电源		固定	DC 故障模型 漂移和振荡	DC 故障模型 漂移和振荡
总线	A.3			
通用	A.7	地址固定	超时	超时
内存管理单元(MMU)	A.8	数据或地址固定	错误的地址解码 MMU 寄存器的软错误导致的地址更改(见注 3 和注 4)	错误的地址解码 MMU 寄存器的软错误导致的地址更改
直接内存访问(DMA)		无或连续访问	数据和地址的 DC 故障模型 DMA 寄存器的软错误导致的信息更改 错误的访问时间	影响内存中数据的所有故障 错误的访问时间
总线仲裁(见注 5)		仲裁信号固定	无或连续仲裁	无、连续或错误的仲裁

表 A.1（续）

元器件	见表	所声明的诊断覆盖率要求		
		低(60%)	中(90%)	高(99%)
中央处理器(CPU) 寄存器，内部RAM	A.4、A.10	数据和地址固定	数据和地址的DC故障模型 软错误导致的信息更改	数据和地址的DC故障模型 内存单元的动态交叉 软错误导致的信息更改 无寻址、错误寻址或多重寻址
编码和执行，包括标志寄存器		错误编码或不执行	错误编码或错误执行	未定义的失效假设
地址计算		固定	DC故障模型 软错误导致的地址更改	未定义的失效假设
程序计数器，堆栈指针		固定	DC故障模型 软错误导致的地址更改	DC故障模型 软错误导致的地址更改
中断处理 中断	A.4	无或连续中断(见注6)	无或连续中断 中断的交叉	无或连续中断 中断的交叉
复位电路		固定 单个元器件未初始化到复位状态	DC故障模型 漂移和振荡 单个元器件未初始化到复位状态	DC故障模型 漂移和振荡 单个元器件未初始化到复位状态
不可变内存	A.5	数据和地址固定	数据和地址的DC故障模型	影响内存中数据的所有故障
可变内存	A.6	数据和地址固定	数据和地址的DC故障模型 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 软错误引起的信息改变 无寻址、错误寻址或多重寻址
时钟(石英、振荡器、锁相环(PLL))	A.11	亚谐波或高次谐波 周期抖动	不正确的频率 周期抖动	不正确的频率 周期抖动
通信和大容量存储器	A.12	错误的数据或地址 不传输	影响内存中数据的所有故障 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	A.13	固定	DC故障模型 漂移和振荡	DC故障模型 漂移和振荡

表 A.1（续）

元器件	见表	所声明的诊断覆盖率要求		
		低(60%)	中(90%)	高(99%)
最终元件	A.14	固定	DC 故障模型 漂移和振荡	DC 故障模型 漂移和振荡

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

注 2：“DC 故障模型”包括的失效模式有：固定(Stuck-at)、固定开(Stuck-open)，开路或高阻抗输出以及信号线间的短路。对于集成电路，任意两个连接(管脚)之间的短路都被视为 DC 故障。

注 3：通常认为，低电压半导体的软错误率(SER)比硬错误率(器件的永久性损坏)高一个数量级(50 倍到 500 倍)。

注 4：软错误的原因是：来自封装中衰变的 α 粒子、中子、外部 EMI 噪声和内部的串扰。软错误的影响只能由运行时的安全完整性措施来把握。针对随机硬件故障的安全完整性措施对软错误未必有效。

示例：内存测试中的漫步路径和跳步模式方法往往是无效的，而使用奇偶校验或 ECC 校验经常性的读内存单元的监视技术或采用比较或表决的冗余技术往往是有效的。

注 5：总线仲裁是一种决定哪个设备具有总线控制权的机制。

注 6：无中断意思是当有一个或多个中断宜发生时，没有发出中断。连续中断的意思是当中断不宜发生时而发出中断。

注 7：对于专用集成电路，此表和表 2～表 18 的相关部分可被适当采用。

表 A.2　电气元器件

诊断技术/措施	见 GB/T 20438.7—2017	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	量化随机故障的影响时宜考虑继电器的开关频率
比较器	A.1.3	高	如果失效模式主要是安全导向，则高
多数表决器	A.1.4	高	依赖于表决质量

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.3　电子元器件

诊断技术/措施	见 GB/T 20438.7—2017	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	如果失效模式主要是安全导向，则高

表 A.3（续）

诊断技术/措施	见 GB/T 20438.7—2017	能达到的最大诊断覆盖率	注
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	依赖于冗余和监视的程度
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—2017	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：有限数量的模版（一个通道）	A.3.1	低	
利用软件进行自测试：漫步位（一个通道）	A.3.2	中	
由硬件支持的自测试（一个通道）	A.3.3	中	
编码处理（一个通道）	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。

注 4：因为很多处理单元的故障会导致控制流的修改，表 A.10 中所列的诊断措施和技术也可以考虑用于处理单元的故障。这些诊断措施和方法只覆盖控制流，不含数据流。

表 A.5　不可变内存范围

诊断技术/措施	见 GB/T 20438.7—2017	能达到的最大诊断覆盖率	注
多位冗余字保护	A.4.1	中	多位冗余字保护的有效性依赖于字地址纳入到多位冗余，并且依赖于各自的措施以检测多位共因故障，例如多重寻址（多行选择、多个局部到全局的位行开关激活），电源供应问题（如电荷泵缺陷），产品的行和列更换（生产产量的措施掩盖了产品故障）等
修改的校验和	A.4.2	低	
单字（8 bit）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（16 bit）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—2017	能达到的最大诊断覆盖率	注
检测板（checkerboard）或跨步（march）RAM 测试法	A.5.1	低	
漫步路径（walk-path）RAM 测试法	A.5.2	中	
跳步模式（galpat）或透明跳步模式（transparent 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	

表 A.6（续）

诊断技术/措施	见 GB/T 20438.7—2017	能达到的最大诊断覆盖率	注
修改的汉明码的 RAM 监视，或利用差错检测和纠错码（EDC）校验数据失效	A.5.6	中	利用修改的汉明码的 RAM 监视，或利用差错检测和纠错码（EDC）校验数据失效的有效性依赖于字地址纳入到汉明码，并且依赖于各自的措施以检测多位共因故障，例如多重寻址（多行选择、多个局部到全局的位行开关激活），产品的行和列更换（生产产量的措施掩盖了产品故障）等
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（例如配置过程）的 RAM，若在每次读/写访问之后执行 GB/T 20438.7—2017 中 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—2017	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
测试模版	A.6.1	高	
代码保护	A.6.2	高	
多通道并行输出	A.6.3	高	仅当诊断测试间隔内数据流改变时才有效
被监视的输出	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
反价的（antivalent）信号传输	A.11.4	高	例如反相信号传输

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—2017	能达到的最大诊断覆盖率	注
1 位硬件冗余	A.7.1	低	在数据路径的多层交叉开关的交换类型中,仅在地址线和控制线被安全措施覆盖时,才能够假设给定的效果
多位硬件冗余	A.7.2	中	在数据路径的多层交叉开关的交换类型中,仅在地址线和控制线被安全措施覆盖时,才能够假设给定的效果
完全硬件冗余	A.7.3	高	
使用测试模版进行检查	A.7.4	高	
传输冗余	A.7.5	高	仅对瞬时故障有效
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—2017	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	
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	

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—2017	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

表 A.10（续）

诊断技术/措施	见 GB/T 20438.7—2017	能达到的最大诊断覆盖率	注
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　时钟

诊断技术/措施	见 GB/T 20438.7—2017	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	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.12　通信和大容量存储器

诊断技术/措施	见 GB/T 20438.7—2017	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	见表 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	见表 A.8	见数据路径/总线

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　传感器

诊断技术/措施	见 GB/T 20438.7—2017	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
模拟信号监视	A.2.7	低	
测试模版	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
正向激励开关	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.14　最终元件(执行器)

诊断技术/措施	见 GB/T 20438.7—2017	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	当量化随机失效影响时,需考虑继电器的开关频率
测试模版	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　系统性安全完整性

下列表给出了有关技术和措施的建议,对应于:

——控制由硬件设计引起的失效(见表 A.15);

——控制由环境应力或影响引起的失效(见表 A.16);

——控制操作过程的失效(见表 A.17);

在表 A.15～表 A.17 中根据安全完整性等级提出的建议和给出的要求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:

——M:在该安全完整性等级下要求采用(强制)的技术或措施。

——HR:在该安全完整性等级下极力推荐的技术或措施。若不使用这种技术或措施,则应详细说明不使用的理由。

——R:在该安全完整性等级下推荐的技术或措施。

—— -:既不推荐也不反对使用的技术或措施。

——NR:在该安全完整性等级下明确不推荐的技术或措施。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:

——低:若使用,采用的技术和措施应在防止系统性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性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性失效方面至少达到高有效性。

表 A.18 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,这在表中通过阴影来表示,具体解释见表。

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。规程的和组织上的技术和措施在整个 E/E/PE 系统安全生命周期中对避免引入故障都是必要的,并且用来测试抵御外界影响的 E/E/PE 安全相关系统行为的确认是必要的,从而证明针对具体应用的内在特性是适当的(见附录 B)。

GB/T 20438.6—2017 的附录 D 给出了共因失效的信息。

注:表 A.15~表 A.17 中的大部分措施均可根据表 A.18 在不同有效性的情况下使用,表 A.18 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.15　用于控制由硬件设计引起的系统性失效的技术和措施

	技术/措施	见 GB/T 20438.7—2017	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
	标准测试访问端口和边界扫描架构	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
	多样化硬件	B.1.4	- 低	- 低	R 中	R 高

要求至少应用一种表中浅灰色阴影组中的技术或 GB/T 20438.3 的表 A.3 中规定的一条技术。

注 1:每一安全完整性等级下面表项的含意,需首先查看本表前的正文。

注 2:这些措施可以根据表 A.18 的使用实现不同的有效性,表 A.18 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 的附录 A,附录 B 和附录 C 给出了和本表相关技术和措施的概述,本表第 2 列为所引用的有关条款。

注 4:对于在低要求运行模式下工作的 E/E/PE 安全相关系统(例如紧急停车系统),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.16　用于控制由环境应力或影响引起的系统性失效的技术和措施

	技术/措施	见 GB/T 20438.7—2017	SIL1	SIL2	SIL3	SIL4
	防电压击穿、电压波动、过压、欠压和其他可能导致危险失效的现象(如交流电源频率变化)的措施	A.8	M 低	M 中	M 中	M 高
	分隔开电力线和信号线(见注 4)	A.11.1	M	M	M	M
	提高抗干扰性	A.11.3	M 低	M 低	M 中	M 高
	抗物理环境(如温度、湿度、水、振动、灰尘、腐蚀物)的措施	A.14	M 低	M 高	M 高	M 高
	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
	空闲电流的原则(当不需要连续控制来达到或保持 EUC 的安全状态时)	A.1.5	R	R	R	R
	检测信号线短路和断路的措施		R	R	R	R
	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
	反价信号传输	A.11.4	R 低	R 低	R 中	R 高
	多样化硬件(见注 6)	B.1.4	- 低	- 低	- 中	R 高
	软件架构	GB/T 20438.3—2017 的 7.4.3	见 GB/T 20438.3—2017 的表 A.2			

此表通过边框中的阴影来分为三个组。在灰色和黑色的阴影组中标有“R”的所有技术可以用本组的其他技术替换,但至少有一个灰色的阴影组的技术和至少一个黑色阴影组的技术被使用。

注 1:每一安全完整性等级下面表项的含意,需首先查看表 A.15 前的正文。

注 2:该表中大部分措施可以根据表 A.18 的使用实现不同的有效性,表 A.18 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—2017 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有关条。

注 4:若信息传输采用光介质,则无需分离电力线和信号线;对于为 E/E/PE 系统的组件供电和为这些组件传送信息而设计的低功率电缆,也无需分离电力线和信号线。

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(例如紧急停车系统),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,硬件充分避免了设计故障并足以防止共因失效,则不需要多样化硬件。

表 A.17　用于控制系统性操作失效的技术和措施

	技术/措施	见 GB/T 20438.7—2017	SIL1	SIL2	SIL3	SIL4
	修改保护	B.4.8	M 低	M 中	M 高	M 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
	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—2017 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，需首先查看表 A.15 前的正文。

注 2：该表中两条措施可以根据表 A.18 的使用实现不同的有效性，表 A.18 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—2017 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有关条。

注 4：对于在低要求运行模式下工作的 E/E/PE 安全相关系统(例如紧急停车系统)，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.18　控制系统性失效的技术和措施的有效性

技术/措施	见 GB/T 20438.7—2017	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)，此硬件可开关一个备用的最终元件	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
标准测试访问端口和边界扫描架构	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
防电源故障、电压波动、过压和欠压的措施	A.8	具有安全关断或切换到备用电源单元的过压保护	具有安全关断或切换到备用电源单元的电压控制(次级)或具有安全关断或切换到备用电源单元的掉电措施

表 A.18（续）

技术/措施	见 GB/T 20438.7—2017	低有效性	高有效性
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	超温探测	通过热保险丝触发安全关闭，或者根据超温的不同等级进行报警和检测，或者进行强制风冷并状态指示
提高抗干扰性（见注）	A.11.3	电源和关键输入输出处的噪声过滤器；需要时加屏蔽	防止未预期电磁侵入的过滤器；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
多样化硬件	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
修改保护	B.4.8	修改需要专用工具	修改需要使用钥匙锁或具有口令保护的专用工具
输入确认	B.4.9	对输入动作向操作者提供反馈	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 A.1.1、A.2.1、A.11.3 和 A.14 的技术时，在技术或措施的高有效性情况下，假设已使用了低有效性的方案。

附 录 B
（规范性附录）
E/E/PE 安全相关系统的技术和措施—在生命周期不同阶段中避免系统性失效

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—2017 的附录 B。在运行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—2017 的附录 A 中作了描述。

要把整个安全生命周期中出现的系统性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：

——系统性故障的影响与引入它的生命周期阶段有关；

——为避免系统性失效的各种单个措施的有效性都与应用有关。

因此，不可能为避免系统性失效进行定量分析。

可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。

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

——由系统安装之后的故障诱发的失效（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：将措施划分为在 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），和在运行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，而避免失效的措施是在安全生命周期过程中实施的。

在表 B.1～表 B.5 中根据安全完整性等级提出的建议和给出的要求，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。重要性表示如下：

——M：在该安全完整性等级下，要求采用（强制）的技术或措施。

——HR：在该安全完整性等级下，极力推荐的技术或措施。若不使用这种技术或措施，则应详细说明不使用的理由。

——R：在该安全完整性等级下，推荐的技术或措施。

—— -：不推荐或不反对使用的技术或措施。

——NR：在该安全完整性等级下，明确不推荐的技术或措施。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：

——低：若使用，采用的技术和措施应在防止系统性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性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性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 在不同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；这在表中通过阴影来表示，具体解释见表。

仅遵从本附录中的指南，并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；

——对生命周期的每个开发阶段，哪些技术和措施是适合的；

——对设计和开发每个特定的 E/E/PE 安全相关系统中遇到的具体问题，哪些技术和措施是最适合的。

表 B.1　在 E/E/PE 系统设计要求规范阶段为避免失误的技术和措施（见 7.2）

	技术/措施	见 GB/T 20438.7—2017	SIL1	SIL2	SIL3	SIL4
	项目管理	B.1.1	M 低	M 低	M 中	M 高
	编制文档	B.1.2	M 低	M 低	M 中	M 高
	分开 E/E/PE 系统安全功能与非安全功能	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—2017 的表 B.7	R 低	R 低	HR 中	HR 高
	检查表	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，但至少需要使用其中的一项技术。

为验证此安全生命周期阶段，至少应使用本表灰色阴影组中或表 B.5 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，需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—2017 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有关条款。

表 B.2　在 E/E/PE 系统设计和开发阶段为避免引入故障的技术和措施(见 7.4)

	技术/措施	见 GB/T 20438.7—2017	SIL1	SIL2	SIL3	SIL4
	遵循指南和标准	B.3.1	M 高	M 高	M 高	M 高
	项目管理	B.1.1	M 低	M 低	M 中	M 高
	编制文档	B.1.2	M 低	M 低	M 中	M 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
	使用经试用证明效果良好(屡试不爽)的元件	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—2017 的表 B.7	R 低	R 低	HR 中	HR 高
	检查表	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—2017 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有关条款。

表 B.3　在 E/E/PE 系统集成阶段为避免故障的技术和措施(见 7.5)

	技术/措施	见 GB/T 20438.7—2017	SIL1	SIL2	SIL3	SIL4
	功能测试	B.5.1	M 高	M 高	M 高	M 高
	项目管理	B.1.1	M 低	M 低	M 中	M 高
	编制文档	B.1.2	M 低	M 低	M 中	M 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—2017 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有关条款。

表 B.4　在 E/E/PE 系统运行和维护规程阶段为避免故障和失效的技术和措施(见 7.6)

	技术/措施	见 GB/T 20438.7—2017	SIL1	SIL2	SIL3	SIL4
	运行和维护说明书	B.4.1	HR 高	HR 高	HR 高	HR 高
	用户友善性	B.4.2	HR 高	HR 高	HR 高	HR 高
	维护友善性	B.4.3	M 低	M 低	M 中	M 高
	项目管理	B.1.1	M 低	M 低	M 中	M 高
	编制文档	B.1.2	HR 低	HR 低	HR 中	HR 高

表 B.4（续）

	技术/措施	见 GB/T 20438.7—2017	SIL1	SIL2	SIL3	SIL4
	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	B.4.6	- 低	R 低	HR 中	HR 高
	仅可由熟练操作员操作	B.4.5	- 低	R 低	R 中	HR 高

表中灰色阴影组中标记“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，应使用检查表（见 GB/T 20438.7—2017 的 B.2.5）或检视（见 GB/T 20438.7—2017 的 B.2.6）。

注 1：每一安全完整性等级下面表项的含义，需首先查看表 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—2017 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有关条款。

表 B.5　在 E/E/PE 系统安全确认阶段为避免故障的技术和措施（见 7.7）

	技术/措施	见 GB/T 20438.7—2017	SIL1	SIL2	SIL3	SIL4
	功能测试	B.5.1	HR 高	HR 高	HR 高	HR 高
	在环境条件下测试功能	B.6.1	HR 高	HR 高	HR 高	HR 高
	浪涌抗扰性测试	B.6.2	HR 高	HR 高	HR 高	HR 高
	故障插入测试（当要求的诊断覆盖率≥90%时）	B.6.10	HR 高	HR 高	HR 高	HR 高
	项目管理	B.1.1	M 低	M 低	M 中	M 高
	编制文档	B.1.2	M 低	M 低	M 中	M 高
	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
	最坏情况分析、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

表 B.5（续）

	技术/措施	见 GB/T 20438.7—2017	SIL1	SIL2	SIL3	SIL4
	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
	最坏情况测试	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，灰色和黑色组中所有标记“R”的技术均是可用该组中的其他技术替换的，但至少需要一项灰色组中的技术(分析技术)和至少需要一项黑色组中的技术(测试技术)。

注 1：每一安全完整性等级下面表项的含义，需首先查看表 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—2017 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 避免系统性失效的技术和措施的有效性

技术/措施	见 GB/T 20438.7—2017	低有效性	高有效性
项目管理(见注)	B.1.1	定义行动和责任；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	独立于设计的确认；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
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；内容检查表；计算机辅助文档管理，形式化变更控制
分开 E/E/PE 安全功能与非安全功能	B.1.3	E/E/PE 安全相关系统和非安全相关系统之间具有良好定义的接口	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

表 B.6（续）

技术/措施	见 GB/T 20438.7—2017	低有效性	高有效性
结构化规范	B.2.1	人工层次化划分至子要求；接口描述	使用计算机辅助工程工具描述层次化划分；自动一致性检查；精细到功能级
形式化方法	B.2.2	由有形式化方法经验的人员使用	由在类似应用中有形式化方法经验的人员借助计算机支持工具使用
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个 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
检查表	B.2.5	为所有安全生命周期阶段准备的检查表；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表
规范的检查	B.2.6	由独立人员进行的安全要求规范检查	由独立组织使用一种能够纠正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	人工进行层次化电路设计	已测试电路部分的复用；在规范、设计、电路图和零部件清单之间的可追溯性；计算机辅助；基于已定义的方法（见 7.4.6）
使用经试用证明效果良好（屡试不爽）的元件（见注）	B.3.3	充分的尺寸富余；结构化特性	经使用证明（见 7.4.10）
模块化（见注）	B.3.4	规模受限的模块；每个模块功能独立	充分证实过的模块的复用；易理解的模块；每个模块最多有一个输入、一个输出和一个失效退出口
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 7.4.10）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	在模块级建模，包括外围单元的边界数据	在元器件级建模，包括边界数据

表 B.6（续）

技术/措施	见 GB/T 20438.7—2017	低有效性	高有效性
硬件的检查	B.3.7	由与设计无关的人员进行检查	由独立组织并使用能够纠正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	由与设计无关的人员进行走查	由独立组织并使用能够纠正发现的所有故障的正式规程进行走查
有限的操作可能性（见注）	B.4.4	用钥匙开关或密码来控制运行模式的改变	已定义的健壮的规程以允许操作
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，并有两年在岗经验	所有操作员每年培训；每个操作员至少具备五年操作较低安全完整性等级的安全设备的经验
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	等价类和输入划分测试，边界值测试，使用预先编制的测试用例	根据因果图，结合在极限运行边界的临界状况，执行测试用例
统计测试（见注）	B.5.3	所有输入数据的统计分布	利用工具获得的测试报告；大量测试用例；根据真实应用情况和假设的失效模型得到的输入数据分布
现场经验（见注）	B.5.4	10 000 h 运行时间；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%；没有安全关键失效	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%；在以往运行中对所有变更（包括不太重要的变更）都有详细的文档记录
浪涌抗扰性测试	B.6.2		可证明浪涌干扰性确实高于实际运行环境的边界值
静态分析	B.6.4	基于方块图；凸显缺陷位置；规定测试用例	基于详细图；在测试用例过程中预测预期行为；使用测试工具
动态分析	B.6.5	基于方块图；凸显缺陷位置；规定测试用例	基于详细图；在测试用例过程中预测预期行为；使用测试工具
失效分析	B.6.6	在模块级，包括外围单元的边界数据	在元件级，包括边界数据

表 B.6（续）

技术/措施	见 GB/T 20438.7—2017	低有效性	高有效性
最坏情况分析	B.6.7	在安全功能上实施分析；对于真实的运行条件使用边界值组合导出	在非安全功能上实施分析；对于真实的运行条件使用边界值组合导出
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（包括罕见情况），都能保持所有安全功能的测试
最坏情况测试	B.6.9	在实际的运行条件中发现的边界值组合下，安全功能仍然能保持的测试	在实际的运行条件中发现的边界值组合下，非安全功能仍然能保持的测试
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	在元器件级包括边界数据
注：在参考 B.1.1、B.1.2、B.3.3、B.3.4、B.4.4、B.4.6、B.5.2、B.5.3、B.5.4、B.6.7 和 B.6.9 的技术时，在技术或措施的高有效性情况下，假设已使用了低有效性的方案。			

附 录 C
（规范性附录）
诊断覆盖率和安全失效分数

C.1 硬件组件的诊断覆盖率和安全失效分数的计算

组件的诊断覆盖率和安全失效分数（见 GB/T 20438.4—2017 中的 3.8.6 和 3.6.15）的计算如下所述：

a) 在没有诊断测试的情况下，进行失效模式与影响分析，以确定组件中的每个元件或元件组的每种失效模式对 E/E/PE 安全相关系统行为的影响。应获取充足的信息（见注 1 和注 2），使之能进行失效模式与影响分析，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 安全相关系统的详细框图，描述组件以及组件与 E/E/PE 安全相关系统中可能影响所考虑的安全功能部分之间的关联。

——组件的硬件示意图，描述每个元件或元件组以及元件间的关系。

——每个元件或元件组的失效模式和失效率，以及与安全和危险失效对应于总失效率的相关百分数。

注 2：本分析要求的严格性依赖于许多因素（见 GB/T 20438.1—2017 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。对于较高的安全完整性等级，失效模式与影响分析将非常依赖于特定的元件类型和应用环境。同样，对于硬件故障裕度为零的硬件架构中使用的组件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；

——危险失效。

c) 在诊断覆盖率和安全失效分数的计算中，不包括无影响失效和无关失效；

d) 通过对每个元件或元件组的失效率（λ）的估算（见注 4），以及失效模式和影响分析的结果，计算出每个元器件或元器件组的安全失效率（λ_S），和危险失效率（λ_D）。当这些失效率之一不是常数时，在 DC 和 SFF 的计算中应使用一个时间段的估算平均值。

注 3：可以使用来自公认的工业数据源，并考虑应用环境因素，估算每一元器件或元器件组的失效率。但最好还是使用具体应用的数据，特别是在组件包含较少数量元器件的情况下，以及在估算某个特定元器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。

e) 对每个元器件或元器件组，估算诊断测试（见 C.2）检测到的危险失效分数，并由此计算诊断测试检测到的危险失效率（λ_{Dd}）。

f) 对于组件，计算总的危险失效率（$\sum\lambda_D$），诊断测试检测到的总的危险失效率（$\sum\lambda_{DD}$），以及总的安全失效率（$\sum\lambda_S$）。

g) 计算组件的诊断覆盖率（$\sum\lambda_{Dd}/\sum\lambda_D$）。

h) 计算组件的安全失效分数：

$$SFF=(\sum\lambda_S+\sum\lambda_{Dd})/(\sum\lambda_S+\sum\lambda_{Dd}+\sum\lambda_{Du})。$$

注 4：当失效率是基于常数失效率时，可以使用上面的公式（见 GB/T 20438.4 中 3.6.15 中指明的公式）。

注 5：在评估每个安全功能避免失效的措施时（见 7.4.5.2），需考虑 E/E/PE 安全相关系统中每个组件的诊断覆盖率（如有的话）。在确定针对硬件安全完整性等级的架构约束时（见 7.4.4），需考虑安全失效分数。

用于确定诊断覆盖率和安全失效分数的分析应覆盖所有的元件，这些元件是确保组件能处理 E/E/PE 安全相关系统要求的安全功能所必需的，包括：电气的、电子的、机电的和机械的等。对于每个元件应考虑所有可能的导致某种非安全状态、当要求响应时阻止一次安全响应或损害 E/E/PE 安全相关

系统的安全完整性的危险失效模式。

表 A.1 列出了在运行期间需检测出的或在推导安全失效分数时需要分析的故障或失效。

如果使用现场数据来支持失效模式与影响分析，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—2017 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：还有一些计算诊断覆盖率的有效替代方法，例如：使用计算机模型的故障仿真。该计算机模型包含 E/E/PE 安全相关系统设计中所用的电路及电子元件（例如在集成电路中细化到晶体管层）的细节。

C.2 确定诊断覆盖率的因素

在计算组件的诊断覆盖率时（见 C.1），应该对每个元件或元件组估算由诊断测试检测到的危险失效部分。对诊断覆盖率有贡献的诊断测试包括，但不限于：

——比较检查，例如冗余信号的监视和比较；

——附加的嵌入式测试，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，例如检测表示传感器失效的超量程值。

为了计算诊断覆盖率，必需确定能被诊断测试检测到的那些失效模式。对简单元件（电阻器、电容器、晶体管等）而言，检测开路或短路的失效可达 100%覆盖率。而对较复杂的 B 类组件（见 7.4.4.1.3）就应考虑到对表 A.1 所示的各种元件的诊断覆盖率的限制。对组件的每个元器件或元器件组以及对 E/E/PE 的安全相关系统的每个组件都应执行这种分析。

注 1：表 A.2～A.14 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。这些测试可以连续或周期的进行（依赖于诊断测试间隔）。这些表并不取代本附录的任何要求。

注 2：诊断测试可以为达到 E/E/PE 安全相关系统的功能安全提供极大帮助。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。

诊断覆盖的计算及其所用的方法，是假设当出现其他的的可被诊断测试检测到的危险故障时，EUC 仍可安全运行。如此假设不成立，则按 E/E/PE 安全相关系统在高要求或连续模式下工作的情况处理（见 7.4.8.3，7.4.5.4 和 7.4.5.4）。

注 3：GB/T 20438.4—2017 的 3.8.6 中给出了诊断覆盖率的定义，诊断覆盖率的一些其他替代定义并不适用于 GB/T 20438。

注 4：用于检测一个组件的危险失效的诊断测试可由 E/E/PE 安全相关系统中的另一组件来实现。

注 5：诊断测试可以连续地也可以间断地进行，这依赖于诊断测试间隔。在有些情况下以及有些时候，诊断测试由于有可能对系统状态产生不利的影响而不能运行。在这种情况下，在计算时可以认为诊断测试没有作用。

附 录 D
（规范性附录）
符合项的安全手册

D.1 总则

符合项的安全手册的目的是，对所有与符合项相关的信息建立文档，以使符合项能够按照GB/T 20438要求集成到安全相关系统、子系统或组件中。

D.2 内容

D.2.1 安全手册应当规定符合项的功能。这些可以用来支持安全相关系统的安全功能、子系统或者组件的功能。规范应明确描述功能和输入输出接口。

对于每一个符合项，安全手册应当包括下列内容：

a) 可执行功能的功能规范；

b) 符合项硬件和/或软件的配置标识，以便按照GB/T 20438.1—2017的6.2.1的要求进行E/E/PE安全相关系统的配置管理；

c) 符合项的使用约束和/或进行符合项的行为分析或失效率分析所基于的假设。

D.2.2 对于每一个功能，安全手册应包括：

a) 由随机硬件失效引发的，导致功能失效的，并且不可通过符合项的内部诊断检测到的符合项的失效模式(依据其输出的行为)；

b) 对a)中每个失效模式，估算出的失效率；

c) 由随机硬件失效引发的，导致功能失效的，并且可以通过符合项的内部诊断检测到的符合项的失效模式(依据其输出的行为)；

d) 由随机硬件失效引发的，导致用于检测功能失效的诊断发生失效的，符合项的内部诊断的失效模式(依据其输出的行为)；

e) 对c)和d)中每个失效模式，估算出的失效率；

f) 对于c)中符合项的内部诊断检测到的每种失效模式，诊断测试间隔；

g) 对于c)中每种失效模式，由内部诊断产生的符合项的输出；

注1：内部诊断的输出可用于产生对E/E/PE安全相关系统、子系统或组件的附加措施(技术/规程)，以实现或保持EUC的安全状态。

h) 任何定期检验测试和/或维护的要求；

i) 对于那些可以被外部诊断检测到的指定功能的失效模式，应该提供足够的信息，以便于外部诊断能力的开发。这些信息应包括详细的失效模式和失效模式的失效率；

j) 硬件故障裕度；

k) 提供功能的符合项的部件的类型A和类型B的划分(见7.4.4.1.2和7.4.4.1.3)。

注2：仅当符合项的应用与EUC危险的关系已知时，失效模式才能被分为安全或危险。例如，如果一个传感器的使用是，高输出信号用于表示EUC的危险(例如高压力)，那么阻止了正确的危险指示(例如输出被固定在低)的失效模式将被列为危险，而导致传感器输出为高的失效模式将被列为安全。这取决于安全相关系统逻辑对传感器信号的解释，因此如果没有对传感器应用方式的约束，则不能进行规定。

此外，符合项声明的诊断覆盖率水平可以根据应用不同而变化，这取决于任何系统逻辑诊断的范围

或外部信号处理对符合项内部诊断的补充。

因此,只有在符合项的应用上具有约束后,才能对硬件故障裕度或安全失效分数进行估算。这些约束是符合项的供应商控制之外的。因此,除非明确规定了由什么构成安全和危险失效模式的基本假设,否则在安全手册中不应声明硬件故障裕度、安全失效分数或任何依赖于安全和危险失效模式认识的其他功能安全特性。

D.2.3 对于符合项的每一个易于发生系统性失效的功能,手册应当包括下列内容:

a) 符合项或为其提供功能的组件部分的系统性能力;

b) 应遵守的,与功能相关的,符合项应用的使用说明或约束,以防止符合项的系统性失效。

注:只有遵守使用说明和约束时,才能够获得由系统性能力表明的系统性安全完整性。如有违反,系统性能力的声明会部分或全部无效。

D.2.4 对于有关软件符合项的附加要求见 GB/T 20438.3—2017 的 7.4.2.12 和附录 D。

附 录 E
（规范性附录）
带片上冗余的集成电路特定架构要求

E.1 概述

本附录在 7.4.2.2b)中被引用。

为了允许在同一个半导体衬底上使用片上冗余，以下给出了一系列要求。出于安全的原因该方法相对保守，例如，它被限制最高到 SIL 3 并且规定一系列限制性要求。以下要求仅与数字集成电路有关。目前对于混合和模拟集成电路还不能给出其通用的要求。对于个别的应用，共因分析（见 GB/T 20438.1—2017 中 7.6.2.7）可能会排除片上冗余的使用。GB/T 20438 中的片上冗余意味着使用双重（或三重）功能单元使硬件故障裕度大于零。根据 7.4.4.1.1a)，在确定硬件故障裕度时，不须考虑可控制故障的影响采取的措施，如：诊断。

可使用单半导体衬底来实现带有硬件故障裕度大于零的子系统（片上冗余）。在这种情况下应履行所有以下要求 a)～q)，并且 E/E/PE 系统和集成电路的设计应满足这些要求。任何带有片上冗余的集成电路应该有其自己的符合项安全手册（见附录 D）。

a) 以上描述的集成电路安全功能可声明的最高安全完整性等级被限制到 SIL 3。

注 1：以目前的技术、知识和经验，考虑和采取相关措施来消除所有影响，让组件（单片集成电路）满足 SIL 4 的要求仍不可行。

b) 不能通过组件的组合来增加系统性能力（见 7.4.3.2）。

c) 为了避免共因失效，需考虑温度升高（如随机的硬件故障引起的）的影响。应至少采用表 E.2 第 6 款的一项措施。在设计中，一个局部故障可能引起一个安全临界温度的增长，应该采取适当的措施。

注 2：在电源的设计中，一个局部故障会引起非常大的温度升高，而逻辑电路的局部短路影响可以被忽略。例如，在数字电路中考虑器件焊盘的面积和稳压器。

d) 应该为集成电路衬底的每个通道和每个监视组件（如看门狗）建立分离的物理块。这些物理块应该包括键合线和引脚。每个通道也应该有它独立的输入和输出，而不应该经过另一个通道/物理块。

注 3：这并不排除块之间的内部连接，以及不同块的输入输出单元之间的连接（见表 E.1 中 3a 和 3b）。

注 4：输入输出包括但不限于：

——DFT 信号（可测试性设计，如：扫描链）；

——时钟信号和时钟使能信号；

——电源；

——复位信号；

——配置和模式选择信号；

——调试和跟踪信号。

e) 应该采取适当措施以避免由于电源故障引起的危险失效，包括共因失效。

注 5：电源故障包括但不限于：

——噪声；

——通过供电线路的扰动传播；

——非同步电源接通，可能引起诸如闩锁效应或高冲击电流等问题；

——短路引起的过度电流消耗；

注 6：本要求可能通过应用以下技术实现，如：

——为每个块提供独立的电源引脚，使得没有一个块的电源供应来自于另一个块（如通过内部连接），并且也不将集成电路中独立物理块的阱连接在一起（见表 E.2 的第 3 条）；

——结合外部措施来避免由阱的不同电压引起的危险失效；

——通过电压监视器检测电源故障；

——使用部分增加的电压容差；

——在电源线路设计中考虑线路压降问题。

f) 独立物理块之间的最小距离应足够，以避免块之间的短路和串扰。

注 7：典型的短路是由于电迁移、通孔迁移、接触迁移、局部有缺陷的栅氧化层被击穿、闩锁效应等引起的。

注 8：典型的串扰是由于衬底电流、电容耦合等引起。

注 9：宜依据设计原则来选择最小间距，典型的安全系数在 10～50。

注 10：当估算独立物理块之间的距离时，表 E.2 中的电势环不被考虑作为块的一部分。

g) 独立物理块相邻线之间的短路和串扰不应该导致安全功能的丧失，或者一个未检测到的监视功能的丧失（表 E.2 的第 5 条）。

h) 无论使用什么集成电路设计工艺，衬底都应该接地（n 阱或 p 阱）。

注 11：对于 p-阱类型工艺，意味着使用负电源。在设计中，宜避免负逻辑，因为它的使用可能容易导致错误。

i) 带有片上冗余的集成电路对于共因失效的敏感性应该通过确定 E.3 中定义的 β 因子来进行评估，该 β 因子被称为 β_{IC}。在集成电路中要使用 β 因子 β_{IC} 来替代根据 GB/T 20438.6—2017 附录 D 中的实例确定的 β 因子，并根据 7.4.5.1 估算 E/E/PE 安全相关系统实现的安全完整性。

j) 带有片上冗余的集成电路检测到故障时（通过诊断测试、检验测试或者其他方法）应该引起特定的行动来实现或保持安全状态。

注 12：本要求并不适用于故障影响可以控制的情况，如：块失电。

k) 每一通道的最小诊断覆盖率应该大于 60%。在监视组件仅被执行一次的场合，该组件的最小诊断覆盖率也应该大于 60%。

l) 如果看门狗是必要的，如：通过程序序列监视和保证必要的诊断覆盖率或安全失效分数，一个通道不应该被用作另一个通道的看门狗，除非使用功能多样化的通道。

m) 当在没有额外安全裕度的情况下测试电磁兼容性时，集成电路执行的功能不应该被干扰（如：在抗电磁干扰标准中描述的性能准则 A，见 GB/T 17799.2 或 IEC 61326-3-1）。

n) 当在有额外安全裕度的情况下测试电磁兼容性时，安全功能（包括集成电路）应该适应定义于 IEC 61326-3-1 中的“FS”准则。

o) 对于连接到外部异步数字信号的数字输入端口，应当采取适当的措施来避免由于振荡而引起的危险失效，如：多级时钟同步的分别引入。

p) 应该分析共用资源的潜在共因，如：边界扫描电路和特殊功能寄存器组等。

q) 以上要求 a）～p）列出的共因引发源主要用于带有片上冗余的集成电路，也应该考虑 GB/T 20438 指定的其他相关共因引发源。

注 13：一般来说，上述要求给出了一种全定制或是半定制片上冗余集成电路设计的限制条件，如：ASIC、微控制器或是其他特定的 SoC（片上系统）。其他的设计如：门电路阵列、FPGA 等可能无法满足所有的要求。

上述带有片上冗余的集成电路只有在完成全部共因分析（CCA）的情况下才能被允许使用。该分析应该覆盖全范围，包括设计、制造、构建、规程和环境因素在内的潜在的共因失效。尤其是由于片上冗余集成电路的使用，通道间的物理隔离的缺失应该接受特别的审查。最终分配给 E/E/PE 安全相关系统的安全完整性等级应该取决于共因分析的结果。

注 14：使用通道间物理隔离可以有效地抵御冗余系统中广泛存在的共模失效；

注 15：推荐的共因分析方法步骤如下：

1) 确定潜在的共因引发源(CCI)。考虑列在附录和其他可预见的物理共因引发源和逻辑引发源(共享资源和信号);
2) 确定集成电路中受共因引发源影响的冗余块;
3) 针对步骤 1 识别的共因引发源和步骤 2 识别的每一对冗余块,定性的列出和评估所采取的安全措施;
4) 定量的回答表 E.1 和 E.2 为步骤 2 确定的每一对冗余块列出的问题,并且评估特定的 β 因子;
5) 在概率建模中使用特定的 β 因子。

E.2 对片上冗余的 SIL3 等级的附加要求

对于片上冗余的 SIL3 等级,除了 E.1 中给出的要求之外,还应满足以下要求:

a) 在规范、分析、验证和确认过程中考虑了所有应用特定环境条件,并提供文件证据。
b) 实现和保持 E/E/PE 系统的安全状态的外部措施。这些外部措施最低应该实现中等有效性(见 A.3)。所有在集成电路内部实现的,用以监视系统性失效和/或共因失效的影响措施,应该使用这些外部措施来实现和保持 E/E/PE 系统的安全状态。

E.3 β 因子

带有片上冗余的集成电路对共因失效的敏感性应该通过确定 β 因子 β_{IC} 来估算,β_{IC} 特定用于片上冗余的集成电路[见 E.1, i)]。估算应基于以下方法:

a) 基本 β 因子称为 $\beta_{B\text{-}IC}$,取值 33%;
b) 使用表 E.1 进行设计,估算基本 β 因子 $\beta_{B\text{-}IC}$ 的增量;
c) 使用表 E.2 进行设计,估算基本 β 因子 $\beta_{B\text{-}IC}$ 的减量。

β_{IC} 通过将 $\beta_{B\text{-}IC}$ 加上表 E.1 所有分数,然后减去表 E.2 所有分数进行估算。β_{IC} 的估算结果不应超过 25%。

注 1:在集成电路中要使用 β 因子 β_{IC} 来替代根据 GB/T 20438.6—2017 附录 D 中的实例确定的 β 因子,并根据 7.4.5.1 估算 E/E/PE 安全相关系统实现的安全完整性。

注 2:宜使用对集成电路设计的可用失效数据的特定分析来证实被选择的 β 因子是保守的。宜仅使用具有成熟的设计和制造工艺的集成电路。

表 E.1 增加 $\beta_{B\text{-}IC}$ 的技术和措施

	技术/措施	β 因子增量(%)	说 明
1	使用片上看门狗作为监视组件	5	用作看门狗功能的监视组件需保证要求的 DC 或 SFF,并且在共因失效的情况下,宜优先考虑在外部实现。与外部实现相比较,片上看门狗的使用可能导致较高的 DC 或 SFF。[见 E.2b)]
2	除看门狗外的其他片上监视组件,如:时钟监视	5	用作时钟监视功能的监控组件需保证要求的 DC 或 SFF,并且在共因失效的情况下,宜优先考虑在外部实现。与外部实现相比较,片上监视组件的使用可能导致较高的 DC 或 SFF。[见 E.2b)]
3a	块之间、独立物理块的输出单元和输入单元之间的内部互连线,没有不同层的交叉	2	独立的物理块之间条件和结果的比较宜优先在集成电路的外部实现。 需要开展可能的共因失效分析,包括内部连接的固定型故障的 FMEA。 由于故障而产生的温度升高尤其要特别予以考虑。 可通过最后布局分析来验证布局,例如可借助工具

表 E.1（续）

	技术/措施	β因子增量(%)	说　明
3b	块之间、独立物理块单元输出单元和输入单元之间的内部互连线有交叉	4	独立的物理块之间条件和结果的比较宜优先在集成电路的外部实现。需要开展可能的共因失效分析，包括内部连接的固定型故障及短路的FMEA。由于故障而产生的温度升高尤其要特别予以考虑

在数字后带有字母的为可选的技术和措施，只能选择其中之一。

本表中列出的技术和措施并不详尽。也可使用其他的技术和措施，给出证据来支持声明的β因子增量。

如果可以提供证据，通过采取相关措施减轻共因失效的影响，也可使用其他β因子增量。在该情形下，应该遵守来自于GB/T 20438.6—2017附录D中的建议。

注：冗余块之间的接口信号通常有多个层组成。不考虑信号的组成，无论它是独立使用一层金属构造，还是它混合多层，整个的接口信号都将被考虑作为一个单线。为了将由于错误引起的干扰降到最低，接口信号间不宜相互交叉。

表 E.2　减少 $\beta_{B\text{-}IC}$ 的技术和措施

	技术/措施	β因子减量(%)	说　明
1a	在不同的通道使用多样化措施控制失效	4	
1b	在不同的通道使用多样化功能和措施控制失效	6	
2	使用额外的安全裕度测试E/E/PE系统的电磁兼容能力，不干扰E/E/PE系统的功能(如：性能准则A)	5	性能准则A描述在抗电磁干扰标准中，见GB/T 17799.2或IEC 61326-3-1
3	为每个块使用独立的电源管脚，使得没有块使用另一个块的电源供应(如：通过内部连接)，并且在集成电路内部独立物理块之间没有连接阱存在	6	应该采取外部措施以避免由于阱的不同电压造成的危险失效
4	结构上使用隔离和去耦的物理位置	2～4	对于解耦独立物理块是有用的
5	在独立物理块的输出引脚之间使用接地引脚	2	如果没有实施，应实施分隔物理块间相邻引线的短路以测试引线键合的撕纸效应[见E.1g)]。在这种情况下，β因子不会降低
6a	每通道诊断覆盖率较高(DC≥99%)，可以在足够短的时间内利用技术过程检测失效并实现安全状态	7	可能仅适用于异常情况
6b	在块之间使用温度传感器，并在足够短的时间内永久关闭(内部或外部)到安全状态；无诊断则低有效性	2	见表A.18，高温采取的措施

表 E.2（续）

	技术/措施	β因子减量(%)	说　明
6c	在块之间使用温度传感器，并在足够短的时间永久关闭(内部或外部)到安全状态；有诊断则高有效性	9	见表 A.18，高温采取措施
6d	分析和测试故障影响(如：增加温度)。取决于分析测试的结果，通道间的比较，包括故障检测和在要求的足够短的时间内实现安全状态	9	
6e	设计温度升高时仍可工作的监视电路	7	在最坏的温度条件下，设计的监视功能(如：看门狗)应该执行安全功能
在数字后带有字母的为可选的技术和措施，仅仅能选择其中之一。 本表中列出的技术和措施并不详尽。也可使用其他的技术和措施，给出证据来支持声明的β因子增量。 **注**：技术/措施 6a～6e 旨在控制由失效引起的温度升高的影响。			

附 录 F
（资料性附录）
ASIC 避免系统性失效的技术与措施

F.1 概述

对于专用集成电路(ASIC)的设计,应使用如下技术和措施来避免 ASIC 开发过程中的失效。

注 1:7.4.6.7 引用了本资料性附录。

注 2:以下的技术和措施仅与数字 ASIC 和用户可编程的 IC 相关。目前对于混合模式和模拟 ASIC 不能给出通用的技术和措施。

a) 所有的设计活动和测试安排,以及用于功能仿真的工具及仿真结果都应该建立文档。

b) 所有的工具、库和制造规程都应该是经使用证明的,包括:

——某个工具在相当长的一段时间内,已在类似或更复杂的项目中应用(包括有相同特性的不同版本)。

注 3:这里说的"相当长一段时间"也许是两年。

——应用通用的或广泛使用的工具来确保能够知道给定工具和/或给定版本可能的缺陷和限制信息,这些在使用的过程应该加以考虑。制造商应实施版本控制和监视以追踪现有的故障。

——内部一致性和可信性的检查,以避免由不同工具创建的不同数据库中的故障。

注 4:用户培训是非常重要的,因为这一领域是快速发展变化的。

c) 需要对所有的活动及其结果进行验证,例如通过仿真、等价性检查、时序分析或者检查技术约束。

d) 应该采用能使设计实施过程可重复和自动化的措施(脚本化、自动化工作和设计实施流程)。

e) 对于第三方提供的软核和硬核,只能使用经确认的宏块,如果可行的话这些宏块应该遵守宏核供应商定义的所有约束和程序。除非已经经使用证明,否则每个宏块都要当做是新写的代码,例如它应该被充分确认。

f) 对设计来说,应该使用面向问题的和抽象的高级设计方法和设计描述语言。

注 5:设计描述宜使用硬件描述语言如 VHDL 或 Verilog。这是当下在 ASIC 设计中最常见的硬件描述方法。这两种语言都是由 IEEE 标准定义,并且假设满足对于高级编程语言的建议。硬件描述语言可以被用于设计描述和功能性建模或测试台。当用于设计描述时,只能使用该语言的一个子集,这种可合成的代码通常被称为 RTL(寄存器传输级)代码。适合于功能性建模和测试台的非可综合代码被称为行为代码。

g) 应该实现充分的可测试性(用于全定制和半定制 ASIC 的制造测试)。

h) 在测试和 ASIC 验证阶段需要考虑门和互连(线)的延迟。

i) 应当尽量避免内部三态输出门。如果使用了内部三态输出,这些输出需要配备上拉/下拉或总线保持器。

j) 在制造之前,整个 ASIC 需要经过充分的验证(即包括在设计和实施过程中完成每个验证步骤,以确保正确的模块和芯片功能)。

注 6:ASIC 验证的充分性取决于组件的测试复杂性和要求的安全完整性等级。

F.2 指南:技术和措施

在 ASIC 的设计和开发过程中应当使用一组适当的技术和措施来阻止故障的引入。根据技术的实

现,有必要分别对待全定制/半定制数字 ASIC 和用户可编程 IC(FPGA/PLD/CPLD)。对于全定制/半定制 ASIC 在表 F.1 中定义了支持实现相关属性的技术和措施,对于用户可编程 IC 在 F.2 中定义。相关的 ASIC 开发生命周期如图 3 所示。

在表 F.1 和表 F.2 中,按照安全完整性等级提出建议,首先指出了技术和措施的重要性,然后是使用该技术时推荐的有效性。重要性表示如下:

——HR*:在该安全完整性等级下,极力推荐的技术或措施。所有的设计都宜用到此项技术或措施。

——HR:在该安全完整性等级下,极力推荐的技术或措施。若不使用这种技术或措施,则应详细说明不使用的理由。

——R:在该安全完整性等级下,推荐的技术或措施。若不使用该项技术或措施或者没有使用可能的替代方法,应详细说明不使用的理由。

——-:不推荐或不反对使用的技术或措施。

——NR:在该安全完整性等级下,明确不推荐的技术或措施。若使用这种技术或措施,则应详细说明使用的理由。

推荐的有效性表示如下:

——低:若使用,采用的技术或措施应在防止系统性失效方面至少达到低有效性。

——中:若使用,采用的技术或措施应在防止系统性失效方面至少达到中有效性。

——高:若使用,采用的技术或措施应在防止系统性失效方面至少达到高有效性。

遵守本附录的指南并不能保证一定能达到要求的安全完整性。重要的是考虑:

——所选择的技术和措施的一致性,以及他们之间互相补充的程度;

——在开发生命周期的每个阶段,适合什么样的技术和措施;

——在每个不同的 E/E/PE 安全相关系统开发的过程中,针对遇到的特定问题哪种技术和措施是最适当的。

表 F.1 ASIC 设计和开发过程中避免引入故障的技术和措施—全定制和半定制的数字 ASIC(见 7.4.6.7)

设计阶段	参考号	技术/措施	见 GB/T 20438.7—2017	SIL 1	SIL 2	SIL 3	SIL 4
设计入口	1	结构化描述	E.3	HR 高	HR 高	HR* 高	HR* 高
	2	(V) HDL 设计描述(见注)	E.1	HR 高	HR 高	HR* 高	HR* 高
	3	原理图输入	E.2	NR	NR	NR	NR
	4	(V) HDL 仿真(见注)	E.5	HR 高	HR 高	HR* 高	HR* 高
	5	应用经使用证明的(V) HDL 仿真器(见注)	E.4	HR 高	HR 高	HR* 高	HR* 高
	6	模块级的功能测试(如:使用(V) HDL 测试平台)(见注)	E.6	HR 高	HR 高	HR* 高	HR* 高

表 F.1（续）

设计阶段	参考号	技术/措施	见 GB/T 20438.7—2017	SIL 1	SIL 2	SIL 3	SIL 4
	7	顶层功能测试	E.7	HR 高	HR 高	HR* 高	HR* 高
	8	嵌入系统环境的功能测试	E.8	R 中	R 中	HR 高	HR 高
	9	异步结构的限制使用	E.9	HR 高	HR 高	HR* 高	HR* 高
	10	主要输入的同步和亚稳态的控制	E.10	HR 高	HR 高	HR* 高	HR* 高
	11	可测性设计(取决于测试覆盖率)	E.11	R ＞95%	R ＞98%	R ＞99%	R ＞99%
	12	模块化	E.12	R 中	R 中	HR 高	HR 高
	13	验证场景的覆盖	E.13	R 中	R 中	HR 高	HR 高
	14	遵循编码指南	E.14	HR 高	HR 高	HR* 高	HR* 高
	15	代码检查器的应用	E.15	R	R	R	R
	16	防御性编程	E.16	R 低	R 中	HR 高	HR* 高
	17	仿真结果建立文档	E.17	HR 低	HR 中	HR 高	HR* 高
	18a	代码审查	E.18	R 中	R 高	HR 高	HR* 高
	18b	走查	E.19	R 中	R 高	HR 高	HR* 高
	19a	已确认软核的应用	E.20	R 中	R 高	HR* 高	HR* 高
	19b	软核的确认	E.21	R 中	R 高	HR* 高	HR* 高
综合	20a	门级网表的仿真来检查时序约束	E.22	R 中	R 中	R 高	R 高
	20b	传播延迟的静态分析(STA)	E.23	R 中	R 中	R 高	R 高

表 F.1（续）

设计阶段	参考号	技术/措施	见 GB/T 20438.7—2017	SIL 1	SIL 2	SIL 3	SIL 4
	21a	对照参考模型，通过仿真验证门级网表	E.24	R 中	R 中	HR 高	HR 高
	21b	比较门级网表和参考模型（形式化等价检查）	E.25	R 中	R 中	HR 高	HR 高
	22	检查 ASIC 供应商的要求和约束	E.26	HR 高	HR 高	HR* 高	HR* 高
	23	综合约束、结果和工具的文档化	E.27	HR 高	HR 高	HR* 高	HR* 高
	24	应用经使用证明的综合工具	E.28	HR* 高	HR* 高	HR* 高	HR* 高
	25	应用经使用证明的目标库	E.29	HR* 高	HR* 高	HR* 高	HR* 高
	26	基于脚本的流程	E.30	R 中	R 中	HR 高	HR 高
测试插入和测试向量生成	27	测试结构的实施	E.31	R >95%	R >98%	R >99%	R >99%
	28a	通过仿真估计测试覆盖率（基于可达到的测试覆盖率）	E.32	R >95%	R >98%	R >99%	R >99%
	28b	通过应用 ATPG 工具估计测试覆盖率（基于可达到的测试覆盖率）	E.33	R >95%	R >98%	R >99%	R >99%
	29a	通过对门级网表的仿真检查时序约束	E.22	R 中	R 中	HR 高	HR 高
	29b	传播延迟的静态分析（STA）	E.23	R 中	R 中	HR 高	HR 高
	30a	对照参考模型，通过仿真验证门级网表	E.24	R 中	R 中	HR 高	HR 高
	30b	比较门级网表和参考模型（形式化等价检查）	E.25	R 中	R 中	HR 高	HR 高

表 F.1（续）

设计阶段	参考号	技术/措施	见 GB/T 20438.7—2017	SIL 1	SIL 2	SIL 3	SIL 4
布局， 布线， 版图生成	31a	对应用的硬核进行经使用证明的论证	E.34	HR 高	HR 高	HR* 高	HR* 高
	31b	应用已确认的硬核	E.35	HR 高	HR 高	HR* 高	HR* 高
	31c	硬核的在线测试	E.36	HR 高	HR 高	HR* 高	HR* 高
	32a	通过对门级网表的仿真检查时序约束	E.22	HR 高	HR 高	HR* 高	HR* 高
	32b	传播延迟的静态分析(STA)	E.23	HR 高	HR 高	HR* 高	HR* 高
	33a	对照参考模型，通过仿真验证门级网表	E.24	HR 高	HR 高	HR* 高	HR* 高
	33b	比较门级网表和参考模型(形式化等价检查)	E.25	HR 高	HR 高	HR* 高	HR* 高
	34	设计规则检查(DRC)	E.37	HR 高	HR 高	HR* 高	HR* 高
	35	版图与原理图对比验证(LVS)	E.38	HR 高	HR 高	HR* 高	HR* 高
	36	应用经使用证明的设计环境和单元库	E.4	HR* 高	HR* 高	HR* 高	HR* 高
	37	对于使用时间小于3年的工艺技术，增加时间裕量(大于20%)	E.39	HR 高	HR 高	HR 高	HR* 高
芯片制造	38	应用经使用证明的工艺技术		HR 高	HR 高	HR* 高	HR* 高
	39	应用经使用证明的制造工艺	E.42	HR 高	HR 高	HR 高	HR* 高
	40	工艺技术的质量保证		HR 高	HR 高	HR 高	HR* 高
	41	制造工艺的质量控制	E.43	HR 高	HR 高	HR 高	HR* 高

表 F.1（续）

设计阶段	参考号	技术/措施	见 GB/T 20438.7—2017	SIL 1	SIL 2	SIL 3	SIL 4
	42	器件的制造质量合格	E.44	R 低	R 中	HR 高	HR* 高
	43	器件的功能质量合格	E.45	HR 高	HR 高	HR 高	HR* 高
	44	制造测试的覆盖率		>95%	>98%	>99%	>99%
	45	质量标准	E.46	HR 高	HR 高	HR 高	HR* 高
	46	质量管理，例如，根据 GB/T 19000		HR 高	HR 高	HR 高	HR* 高
	47	老化测试	E.40	R 低	R 中	HR 高	HR* 高
根据安全完整性等级来选择适当的技术或措施。替代的或等效的技术和措施由一个数字后带字母指示。至少有一个可以替代的或等效的技术或措施。 **注**：术语（V)HDL 是指高速集成电路硬件描述语言或 Verilog 硬件描述语言。							

表 F.2　ASIC 的设计实现过程中避免引入故障的技术和措施—用户可编程 IC(FPGA/PLD/CPLD)（见 7.4.6.7）

设计阶段	参考号	技术/措施	见 GB/T 20438.7—2017	SIL 1	SIL 2	SIL 3	SIL 4
设计入口	1	结构化描述	E.3	HR 高	HR 高	HR* 高	HR* 高
	2	（V）HDL 设计描述(见注)	E.1	HR 高	HR 高	HR* 高	HR* 高
	3	原理图输入	E.2	- 高	- 高	NR	NR
	4	使用布尔方程式进行设计描述		R 高	R 高	NR	NR
	5a	对于使用布尔方程式进行描述的电路：对有限(低)复杂度设计采用人工审查		HR 高	HR 高	HR* 高	HR* 高
	5b	对于使用布尔方程式进行描述的电路：对较高复杂度设计采用状态转换的仿真		HR 高	HR 高	HR* 高	HR* 高

表 F.2（续）

设计阶段	参考号	技术/措施	见 GB/T 20438.7—2017	SIL 1	SIL 2	SIL 3	SIL 4
	6	应用经使用证明的设计环境	E.4	HR 高	HR 高	HR* 高	HR* 高
	7	应用经使用证明的(V)HDL 仿真器(见注)	E.4	HR 高	HR 高	HR* 高	HR* 高
	8	模块级的功能测试(例如：使用(V)HDL 测试平台)(见注)	E.6	HR 高	HR 高	HR* 高	HR* 高
	9	异步结构的限制使用	E.9	HR 高	HR 高	HR* 高	HR* 高
	10	可测试性设计(取决于测试覆盖率)	E.11	R >95%	R >98%	R >99%	R >99%
	11	模块化	E.12	R 中	R 中	HR 高	HR 高
	12	验证场景的覆盖(测试平台)	E.13	R 中	R 中	HR 高	HR 高
	13	遵循编码指南	E.14	HR 高	HR 高	HR* 高	HR* 高
	14	仿真结果建立文档	E.17	HR 低	HR 中	HR 高	HR* 高
	15a	代码检查	E.18	HR 中	HR 高	HR 高	HR* 高
	15b	走查	E.19	R 中	R 高	HR 高	HR* 高
	16a	经过确认的软核的应用	E.20	R 中	R 高	HR 高	HR* 高
	16b	软核确认	E.21	R 中	R 高	HR* 高	HR* 高
综合	17	内部一致性检查(见 GB/T 20438.7—2017 的 E.4)		HR 高	HR 高	HR* 高	HR* 高
	18a	仿真门级网表来检查时序约束	E.22	R 中	R 中	R 高	R 高

表 F.2（续）

设计阶段	参考号	技术/措施	见 GB/T 20438.7—2017	SIL 1	SIL 2	SIL 3	SIL 4
	18b	传播延迟的静态分析	E.23	R 中	R 中	R 高	R 高
	19a	用仿真验证门级网表和参考模型是否一致	E.24	R 中	R 中	HR 高	HR 高
	19b	比较门级网表和参考模型(形式化等价检查)	E.25	R 中	R 中	HR 高	HR 高
	20	对于复杂设计中的 PLD/CPLD：通过仿真来检查设计		R 中	R 中	HR 高	HR 高
	21	检查 IC 供应商的要求和约束	E.26	HR 高	HR 高	HR* 高	HR* 高
	22	综合约束、结果和工具的文档化	E.27	HR 高	HR 高	HR* 高	HR* 高
	23	应用经使用证明的综合工具	E.28	HR 高	HR 高	HR* 高	HR* 高
	24	应用经使用证明的库/CPLD 工艺	E.29	HR 高	HR 高	HR* 高	HR* 高
	25	基于脚本的流程	E.30	R 高	R 高	HR 高	HR* 高
布局， 布线， 版图生成	26a	对应用的硬核进行经使用证明的论证	E.34	HR 高	HR 高	HR* 高	HR* 高
	26b	应用已确认的硬核	E.35	HR 高	HR 高	HR* 高	HR* 高
	26c	硬核的在线测试	E.36	HR 高	HR 高	HR* 高	HR* 高
	27a	通过对门级网表的仿真检查时序约束	E.22	HR 高	HR 高	HR* 高	HR* 高
	27b	传播延迟的静态分析(STA)	E.23	HR 高	HR 高	HR* 高	HR* 高
	28a	通过仿真来验证门级网表和参考模型的一致性	E.24	HR 高	HR 高	HR* 高	HR* 高

表 F.2（续）

设计阶段	参考号	技术/措施	见 GB/T 20438.7—2017	SIL 1	SIL 2	SIL 3	SIL 4
	28b	比较门级网表和参考模型(形式化等价检查)	E.25	HR 高	HR 高	HR* 高	HR* 高
	29	设计规则检查(DRC)	E.37	HR 高	HR 高	HR 高	HR* 高
	30	应用经使用证明的设计环境,应用经使用证明的单元库	E.4	HR* 高	HR* 高	HR* 高	HR* 高
	31	对于使用时间小于 3 年的工艺技术,增加时间裕量(大于 20%)	E.39	HR 高	HR 高	HR* 高	HR* 高
制造	32	应用经使用证明的工艺技术		HR 高	HR 高	HR* 高	HR* 高
	33	应用经使用证明的器件系列	E.41	HR 高	HR 高	HR* 高	HR* 高
	34	经使用证明的制造工艺	E.42	HR 低	HR 中	HR 高	HR* 高
	35	制造工艺的质量控制	E.43	HR 高	HR 高	HR 高	HR* 高
	36	器件的制造质量合格	E.44	R 低	R 中	HR 高	HR* 高
	37	器件的功能质量合格	E.45	HR 高	HR 高	HR* 高	HR* 高
	38	质量标准	E.46	HR 高	HR 高	HR 高	HR* 高
	39	质量管理,例如,根据 GB/T 19000		HR 高	HR 高	HR 高	HR* 高
	40	系统中 FPGA/PLD 原型的最终验证和确认		HR 高	HR 高	HR* 高	HR* 高
	41	在大规模生产和单元检查中的最终验证和确认		R 高	R 高	HR* 高	HR* 高
	42	老化测试	E.40	R 低	R 低	R 中	HR* 高

根据安全完整性等级来选择适当的技术或措施。替代的或等效的技术和措施由一个数字后带字母指示。至少有一个可以替代的或等效的技术或措施。

注：术语（V)HDL 是指高速集成电路硬件描述语言或 Verilog 硬件描述语言。

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

[4] 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

[5] GB/T 20438.6—2017 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

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

[7] IEC 61165 Application of Markov techniques

[8] IEC 61078 Analysis techniques for dependability—Reliability block diagram and boolean methods

[9] IEC 61164 Reliability growth—Statistical test and estimation methods

[10] IEC 62308 Equipment reliability—Reliability assessment methods

[11] GB/T 17799.2 电磁兼容 通用标准 工业环境中的抗扰度试验

[12] GB/T 20172 石油天然气工业 设备可靠性和维修数据的采集与交换

[13] GB/T 2900.13 电工术语 可信性与服务质量

[14] GB/T 19000 质量管理体系 基础和术语

[15] IEC 60300-3-2 Dependability management—Part 3-2: Application guide—Collection of dependability data from the field

[16] IEEE 352:1987 IEEE guide for general principles of reliability analysis of nuclear power generating station safety systems

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—2017/IEC 61508-2:2010
*
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:155066·1-57432

GB/T 20438.2-2017