



中华人民共和国国家标准

GB/T 20438.6—2006/IEC 61508-6:2000

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

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

(IEC 61508-6:2000, IDT)

2006-07-25 发布

2007-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会

发布

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	3
3 定义和缩略语	3
附录 A (资料性附录) GB/T 20438.2 和 GB/T 20438.3 的应用	4
附录 B (资料性附录) 硬件失效概率评估技术示例	11
附录 C (资料性附录) 诊断覆盖率和安全失效分数的计算:工作示例	38
附录 D (资料性附录) 量化 E/E/PE 系统中硬件共同原因失效效应的方法	41
附录 E (资料性附录) GB/T 20438.3 中软件安全完整性表的应用示例	50
参考文献	59
表 B.1 本附录中使用的术语及其范围(应用于 1001、1002、2002、1002D、2003)	13
表 B.2 检验测试时间间隔为 6 个月、平均恢复时间 8 h 时要求的平均失效概率	19
表 B.3 检验测试时间间隔为 1 年、平均恢复时间为 8 h 时要求的平均失效概率	20
表 B.4 检验测试时间间隔为 2 年、平均恢复时间为 8 h 时要求的平均失效概率	22
表 B.5 检验测试时间间隔为 10 年、平均恢复时间为 8 h 时要求的平均失效概率	24
表 B.6 低要求操作模式示例中传感器子系统在要求时的平均失效概率(检验测试时间间隔为 1 年, $MTTR$ 为 8 h)	26
表 B.7 低要求操作模式示例中逻辑子系统在要求时的平均失效概率(检验测试时间间隔为 1 年, $MTTR$ 为 8 h)	26
表 B.8 低要求操作模式示例中最终元件子系统在要求时的平均失效概率(检验测试时间间隔为 1 年, $MTTR$ 为 8 h)	26
表 B.9 不完善检验测试的示例	27
表 B.10 检验测试时间间隔为 1 个月,平均恢复时间为 8 h 时每小时的平均失效概率	29
表 B.11 检测测试时间间隔为 3 个月,平均恢复时间为 8 h 时每小时的平均失效概率	30
表 B.12 检验测试时间间隔为 6 个月,平均恢复时间为 8 h 时每小时的平均失效概率	32
表 B.13 检验测试时间间隔为 1 年以及平均恢复时间为 8 h 时每小时的平均失效概率	33
表 B.14 高要求或连续操作模式结构示例中传感器子系统每小时的失效概率	36
表 B.15 高要求或连续操作模式结构示例中逻辑子系统每小时的失效概率	36
表 B.16 高要求或连续操作模式结构示例中最终元件子系统每小时的失效概率	36
表 C.1 计算诊断覆盖率和安全失效分数示例	39
表 C.2 不同子系统的诊断覆盖率和有效性	40
表 D.1 可编程电子或传感器或最终元件的评分	45
表 D.2 Z 的值:可编程电子	47
表 D.3 Z 的值:传感器或最终元件	48
表 D.4 β 和 β_D 的计算	48
表 D.5 可编程电子的示例值	49

表 E.1	软件安全要求规范(见 GB/T 20438.3—2006 的 7.2)	51
表 E.2	软件设计与开发:软件结构设计(见 GB/T 20438.3—2006 的 7.4.3)	51
表 E.3	软件设计与开发:支持工具和编程语言(见 GB/T 20438.3—2006 的 7.4.4)	52
表 E.4	软件设计与开发:详细设计(见 GB/T 20438.3—2006 的 7.4.5 及 7.4.6)	52
表 E.5	软件设计与开发:软件模型测试和集成(见 GB/T 20438.3—2006 的 7.4.7 及 7.4.8)	52
表 E.6	可编程电子集成(硬件和软件)(见 GB/T 20438.3—2006 的 7.5)	53
表 E.7	软件安全确认(见 GB/T 20438.3—2006 的 7.7)	53
表 E.8	软件修改(见 GB/T 20438.3—2006 的 7.8)	53
表 E.9	软件验证(见 GB/T 20438.3—2006 的 7.9)	54
表 E.10	功能安全评估(见 GB/T 20438.3—2006 的第 8 章)	54
表 E.11	软件安全要求规范(见 GB/T 20438.3—2006 的 7.2)	55
表 E.12	软件设计与开发:软件结构设计(见 GB/T 20438.3—2006 的 7.4.3)	55
表 E.13	软件设计与开发:支持工具及编程语言(见 GB/T 20438.3—2006 的 7.4.4)	56
表 E.14	软件设计与开发:详细设计(见 GB/T 20438.3—2006 的 7.4.5 和 7.4.6)	56
表 E.15	软件设计与开发:软件模块测试和集成(见 GB/T 20438.3—2006 的 7.4.7 和 7.4.8)	56
表 E.16	可编程电子集成(硬件和软件)(见 GB/T 20438.3—2006 的 7.5)	57
表 E.17	软件安全确认(见 GB/T 20438.3—2006 的 7.7)	57
表 E.18	修改(见 GB/T 20438.3—2006 的 7.8)	57
表 E.19	软件的确认(见 GB/T 20438.3—2006 的 7.9)	58
表 E.20	功能安全评估(见 GB/T 20438.3—2006 的第 8 章)	58
图 1	GB/T 20438 的总体框架	2
图 A.1	GB/T 20438.2 的应用	6
图 A.2	GB/T 20438.2 的应用	7
图 A.3	GB/T 20438.3 的应用	9
图 B.1	两个传感器通道配置示例	12
图 B.2	子系统结构	15
图 B.3	1oo1 物理块图	15
图 B.4	1oo1 可靠性块图	16
图 B.5	1oo2 物理块图	16
图 B.6	1oo2 可靠性块图	17
图 B.7	2oo2 物理块图	17
图 B.8	2oo2 可靠性块图	17
图 B.9	1oo2D 物理块图	18
图 B.10	1oo2D 可靠性块图	18
图 B.11	2oo3 物理块图	18
图 B.12	2oo3 可靠性块图	19
图 B.13	低要求操作模式结构示例	25
图 B.14	高要求或连续操作模式的结构示例	35
图 D.1	各个通道失效与共同原因失效的关系	42

前 言

GB/T 20438 由下列 7 部分构成：

- 第 1 部分：一般要求；
- 第 2 部分：电气/电子/可编程电子安全相关系统的要求；
- 第 3 部分：软件要求；
- 第 4 部分：定义和缩略语；
- 第 5 部分：确定安全完整性等级的方法示例；
- 第 6 部分：GB/T 20438.2 和 GB/T 20438.3 的应用指南；
- 第 7 部分：技术和措施概述。

本部分是 GB/T 20438 的第 6 部分。

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

附录 A、附录 B、附录 C、附录 D、附录 E 为资料性附录。

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

- a) 将“IEC 61508”改为“GB/T 20438”。
- b) “本国际标准”一词改为“本标准”。
- c) 删除国际标准中 1.3 的注，因为此注所表述的是 IEC 61508 在美国和加拿大等国的应用情况，与我国的实际不符，所以删除。
- d) 用小数点“.”代替原标准中作为小数点的逗号“，”。

本部分由中国机械工业联合会提出。

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

本部分由机械工业仪器仪表综合技术经济研究所负责起草。

本部分主要起草人：郑旭、冯晓升、梅格、王莉、欧阳劲松等。

引 言

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

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

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

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

GB/T 20438

- 考虑了当使用 E/E/PES 执行安全功能时,所涉及到的整体安全生命周期、E/E/PES 安全生命周期以及软件安全生命周期的各阶段(如初始构思,整个设计、实现、运行、维护及停用)。
- 针对飞速发展的技术,建立一个足够健壮而广泛的能满足今后发展需要的框架。
- 有利于促进 E/E/PE 安全相关系统在不同领域中相关标准的制订,各应用领域和交叉应用领域相关标准应在 GB/T 20438 的框架下制定,使之具有高水平的一致性(如基础原理,术语等的一致性)并将既安全又经济。
- 为达到 E/E/PE 安全相关系统所需的功能安全,提供了编制安全要求规范的方法。
- 使用了一个安全完整性等级,此安全完整性等级规定了 E/E/PE 安全相关系统要实现的安全功能的目标安全完整性等级。
- 采用了一种基于风险的方案来确定安全完整性等级要求。
- 建立了 E/E/PE 安全相关系统的数值目标失效量,这些量都同安全完整性等级相联系。
- 建立了危险失效模式中目标失效量的一个下限,此下限是对单一 E/E/PE 安全相关系统的要求。

这些系统运行在:

- 1) 低要求操作模式下,为了执行它的设计功能,一旦要求时,就把下限设定成平均失效概率为 10^{-5} ;
- 2) 高要求操作模式或者连续操作模式下,下限设定成危险失效概率为 $10^{-9}/h$ 。

注:单一 E/E/PE 安全相关系统不一定是单通道结构。

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

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

1 范围

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

- 附录 A 中阐述了 GB/T 20438.2 及 GB/T 20438.3 的要求简述,以及应用过程中的功能步骤。
- 附录 B 列举了如何计算硬件失效概率。阅读时要结合 GB/T 20438.2—2006 的 7.4.3 和附录 C 以及本部分的附录 D。
- 附录 C 给出了诊断覆盖率的计算示例,阅读时要结合 GB/T 20438.2—2006 的附录 C。
- 附录 D 阐述了将硬件共同原因失效率量化的方法论。
- 附录 E 给出了 GB/T 20438.3—2006 附录 A 中规定的在安全完整性等级 2 和 3 时软件安全完整性表的应用示例。

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

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

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