ICS 25.040
N 10

中华人民共和国国家标准

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

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

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

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

2017-12-29 发布　　2018-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中 华 人 民 共 和 国
国 家 标 准
电气/电子/可编程电子安全相关系统的功能安全 第6部分：GB/T 20438.2和GB/T 20438.3的应用指南
GB/T 20438.6—2017/IEC 61508-6：2010
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址：www.spc.org.cn
服务热线：400-168-0010
2017年11月第一版
*
书号：155066·1-57856

目　　次

前　言

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

——第1部分：一般要求；

——第2部分：电气/电子/可编程电子安全相关系统的要求；

——第3部分：软件要求；

——第4部分：定义和缩略语；

——第5部分：确定安全完整性等级的方法示例；

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

——第7部分：技术和措施概述。

本部分为GB/T 20438的第6部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 20438.6—2006《电气/电子/可编程电子安全相关系统的功能安全　第6部分：GB/T 20438.2和GB/T 20438.3的应用指南》，与GB/T 20438.6—2006相比，主要技术变化如下：

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

——增加了不同结构共因失效因子的方法(见附录D.7)。

本部分使用翻译法等同采用IEC 61508-6:2010《电气/电子/可编程电子安全相关系统的功能安全　第6部分：IEC 61508-2和IEC 61508-3的应用指南》。

本部分做了下列编辑性修改：

——为与现有标准系列一致，将标准名称改为《电气/电子/可编程电子安全相关系统的功能安全　第6部分：GB/T 20438.2和GB/T 20438.3的应用指南》

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

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

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

本部分所代替标准的历次版本发布情况为：

——GB/T 20438.6—2006。

引　言

由电气和电子器件构成的系统，多年来在许多应用领域中执行其安全功能。以计算机为基础的系统（一般指可编程电子系统）在其应用领域中用于执行非安全功能，并且也越来越多地用于执行安全功能。如果要安全并有效地使用计算机技术，有关决策者在安全方面有充足的指导并据此做出决定是十分必要的 。

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

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

在许多情况下，可用多种基于不同技术（如机械的、液压的、气动的、电气的、电子的、可编程电子的等）的系统来保证安全。因而不得不考虑各类安全策略，不仅要考虑单个系统中的所有组件的问题（如传感器、控制器、执行器等），还要考虑不同安全相关系统组合后的问题。因此当 GB/T 20438 在关注电气/电子/可编程电子（E/E/PE）安全相关系统的同时，也提供了一个框架，在这个框架内，基于其他技术的安全相关系统也可被考虑进去。

在各种应用领域里，存在着许多潜在的危险和风险，包含的复杂性也各不相同，从而需应用不同的 E/E/PE 安全相关系统。对每个特定的应用，根据特定应用的许多因素来确定所需的安全措施。GB/T 20438 作为基本原则可在未来的产品和应用领域国家标准制定和已有标准的修订中规范这些措施。

GB/T 20438

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

——针对飞速发展的技术，建立一个足够健全且广泛满足未来发展需求的框架；

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

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

——采用了一种可确定安全完整性要求的基于风险的方法；

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

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

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

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

——低要求运行模式下，下限设定成要求时危险失效平均概率为 10^{-5}；

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

注 3：单一 E/E/PE 安全相关系统不一定是单通道架构。

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

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

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

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

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

1　范围

1.1　GB/T 20438的本部分包括GB/T 20438.2与GB/T 20438.3的信息以及指南。

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

——附录B列举了如何计算硬件失效概率。阅读时要结合GB/T 20438.2—2017的7.4.3、附录C和本部分的附录D。

——附录C给出了诊断覆盖率的计算示例,阅读时要结合GB/T 20438.2—2017的附录C。

——附录D阐述了将硬件共因失效率量化的方法。

——附录E给出了GB/T 20438.3—2017附录A中规定的在安全完整性等级2和3时软件安全完整性表的应用示例。

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

1.3　技术委员会的职责之一就是只要合适,在制定其标准时都应使用基础安全标准。也就是说,本基础安全标准涉及的要求、测试方法或测试条件,只有在相关技术委员会制定标准时加以引用或包含时才能得到应用。

1.4　图1表示了GB/T 20438的整体框架,同时明确了本部分在实现E/E/PE安全相关系统功能安全过程中的作用。