ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.7—2006/IEC 61508-7:2000

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

Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 7:Overview of techniques and measures

(IEC 61508-7:2000,IDT)

2006-07-25 发布　　2007-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中 华 人 民 共 和 国
国 家 标 准
电气/电子/可编程电子安全相关系统的
功能安全 第7部分:技术和措施概述
GB/T 20438.7—2006/IEC 61508-7:2000
*
中国标准出版社出版发行
北京西城区复兴门外三里河北街16号
邮政编码:100045
http://www.spc.net.cn
电话:(010)51299090、68522006
2007年2月第一版
*
书号:155066·1-28713

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 7 部分。

本部分等同翻译国际标准 IEC 61508-7:2000-03(第 1 版)《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》(英文版)。

附录 A、附录 B、附录 C、附录 D 为资料性附录。

本部分与 IEC 61508-7:2000 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：欧阳劲松、冯晓升、王莉、蔡廷安、马光武、梅恪、郑旭等。

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7部分:技术和措施概述

1 范围

1.1 GB/T 20438的本部分包含了GB/T 20438.2和GB/T 20438.3有关的各种安全技术和措施的概述。

注:参考文献仅作为各种方法和工具或示例的基本参考,不一定代表当前技术水平。

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的3.4.4),但作为基础安全标准,各技术委员会可以在IEC导则104和ISO/IEC导则51的指导下制定相关标准时使用。对于每个技术委员会,都有责任在其制定的标准中使用基础标准。同时,GB/T 20438也是一个可独立使用的标准。

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:只有在满足所有有关要求时,才能实现E/E/PE安全相关系统的功能安全,因此,仔细考虑和适当参考所有有关要求是很重要的。

1.3 图1是GB/T 20438的整体框架图,并指出了GB/T 20438.7在实现E/E/PE安全相关系统功能安全中所起的作用。