ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.3—2006/IEC 61508-3:1998

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

Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 3: Software requirements

(IEC 61508-3:1998,IDT)

2006-07-25 发布　　2007-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 20438 由下列 7 部分构成：

——第 1 部分：一般要求；

——第 2 部分：电气/电子/可编程电子安全相关系统的要求；

——第 3 部分：软件要求；

——第 4 部分：定义和缩略语；

——第 5 部分：确定安全完整性等级的方法示例；

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

——第 7 部分：技术和措施概述。

本部分是 GB/T 20438 的第 3 部分。

本部分等同采用国际标准 IEC 61508-3:1998《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》(英文版)。

本部分的附录 A、附录 B 为规范性附录。

本部分与 IEC 61508-3:1998 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 的注 2，因为此注所表述的是 IEC 61508 在美国和加拿大等国的应用情况，与我国的实际不符，所以删除。

d) 用小数点“.”代替作为小数点的逗号“,”。

本部分由中国机械工业联合会提出。

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

本部分由机械工业仪器仪表综合技术经济研究所负责起草。

本部分主要起草人：王莉、冯晓升、梅恪、郑旭、欧阳劲松等。

引　言

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

GB/T 20438 针对由电气或电子和可编程电子部件构成的、起安全作用的电气/电子/可编程电子系统（E/E/PES）的整体安全生命周期，提出了一个通用的方法。建立统一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3部分:软件要求

1　范围

1.1　GB/T 20438的本部分:

a)　使用应建立在充分理解GB/T 20438.1、GB/T 20438.2的基础上。

b)　适用于任何在GB/T 20438.1、GB/T 20438.2范围内构成与安全相关系统的一部分有关的或用于开发安全相关系统的软件。这种软件定义为安全软件。

——安全软件包括操作系统、系统软件、通信网络中的软件、人机界面功能、支持工具、固件以及应用程序。

——应用程序包括高级语言、低级语言程序和使用有限可变语言的特殊用途程序(见GB/T 20438.4—2006的3.2.7)。

c)　软件安全功能和软件安全完整性等级的要求应明确。

注1:如果这一要求作为电气/电子/可编程安全相关系统(见GB/T 20438.2—2006的7.2)有一部分已提出,则在此处不需重复。

注2:规定软件安全功能和软件安全完整性等级是一个重复的程序,见图2和图6。

注3:文档结构要求见GB/T 20438.1—2006的第5章和GB/T 20438.1—2006的附录A。文档结构应考虑公司规程和特殊应用领域的工作实际情况。

d)　建立安全生命周期阶段和在设计、开发与安全有关的软件(软件安全生命周期软件模块)阶段和行为的要求。这些要求包括根据安全完整性等级分等的、在软件中用于避免和控制故障及失效的措施和技术的应用。

e)　对向执行电气/电子/可编程集成的机构提供与软件安全性确认有关的信息提出要求。

f)　对操作和维护E/E/PE安全相关系统的用户所需的与软件有关的信息和规程的准备提出要求。

g)　对修改与安全有关的软件的机构提出要求。

h)　结合GB/T 20438.1、GB/T 20438.2提出对支持工具的要求,如设计开发工具、语言翻译器、测试和调试工具、配置管理工具。

注4:图4和图6表示了GB/T 20438.2和GB/T 20438.3之间的关系。

1.2　GB/T 20438.1、GB/T 20438.2、GB/T 20438.3和GB/T 20438.4是基础的安全标准,尽管它们不适用于简单E/E/PE安全相关系统(见GB/T 20438.4—2006的3.4.4),作为基础的安全标准,根据IEC导则104和ISO/IEC导则51中包含的原则,各技术委员会在起草标准时应考虑使用这些标准,因为技术委员会的责任之一是在起草自己标准时凡是适用之处都应贯彻基础安全标准。GB/T 20438同时也可作为独立的标准去使用。

1.3　图1表示了GB/T 20438的整体框架同时明确了在达到E/E/PE安全相关系统功能安全阶段中本部分的作用。GB/T 20438.6—2006的附录A描述了GB/T 20438.2和GB/T 20438.3的应用。

2　规范性引用文件

下列文档中的条款通过GB/T 20438的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。