ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.1—2006/IEC 61508-1:1998

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

Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 1:General requirements

(IEC 61508-1:1998,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 …… 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
4　与 GB/T 20438 的符合性 …… 3
5　文档 …… 4
5.1　目的 …… 4
5.2　要求 …… 4
6　功能安全的管理 …… 4
6.1　目的 …… 4
6.2　要求 …… 5
7　整体安全生命周期的要求 …… 6
7.1　一般要求 …… 6
7.2　概念 …… 13
7.3　整体范围定义 …… 13
7.4　危险和风险分析 …… 13
7.5　整体安全要求 …… 14
7.6　安全要求分配 …… 16
7.7　整体操作和维护计划编制 …… 19
7.8　整体安全确认计划编制 …… 20
7.9　整体安装和试运行计划编制 …… 21
7.10　实现:E/E/PES …… 21
7.11　实现:其他技术 …… 21
7.12　实现:外部风险降低设施 …… 21
7.13　整体安装和试运行 …… 22
7.14　整体安全确认 …… 22
7.15　整体操作、维护和修理 …… 22
7.16　整体修改和改型 …… 24
7.17　停用或处理 …… 25
7.18　验证 …… 26
8　功能安全评估 …… 26
8.1　目的 …… 26
8.2　要求 …… 26
附录 A（资料性附录）　文档结构范例 …… 29
附录 B（资料性附录）　人员能力 …… 34
参考文献 …… 35

图 1　GB/T 20438 的总体框架 …… 2
图 2　整体安全生命周期 …… 6
图 3　E/E/PES 安全生命周期(实现阶段) …… 7
图 4　软件安全生命周期(实现阶段) …… 8
图 5　E/E/PES 整体安全生命周期和软件安全生命周期之间的关系 …… 8
图 6　对 E/E/PE 安全相关系统、其他技术安全相关系统和外部风险降低设施的安全要求的分配 …… 17
图 7　操作和维护活动模型示例 …… 23
图 8　操作和维修管理模型示例 …… 24
图 9　修改规程模型示例 …… 25
图 A.1　把信息构建成用户群的文档集 …… 32
图 A.2　大型复杂系统和小型简单系统的结构化信息 …… 33

表 1　整体安全生命周期:概述 …… 9
表 2　安全完整性等级:在低要求操作模式下分配给一个 E/E/PE 安全相关系统的安全功能目标失效量 …… 18
表 3　安全完整性等级:在高要求或连续操作模式下分配给一个 E/E/PE 安全相关系统的安全功能目标失效量 …… 18
表 4　执行功能安全评估各方的最低独立水平[包括整体安全生命周期阶段 1～8 和 12～16(见图 2)] …… 28
表 5　进行功能安全评估各方的最低独立水平[整体安全生命周期阶段 9，包括 E/E/PES 安全生命周期和软件安全生命周期的所有阶段(见图 2,图 3 和图 4)] …… 28
表 A.1　与整体安全生命周期有关信息的文档结构示例 …… 30
表 A.2　与 E/E/PES 安全生命周期有关信息的文档结构示例 …… 30
表 A.3　与软件安全生命周期有关的信息文档结构示例 …… 31

前　言

GB/T 20438 由下列几部分构成：

——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 1 部分。

本部分等同采用国际标准 IEC 61508-1:1998《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》(英文版)。

本部分的附录 A、附录 B 为资料性附录。

本部分与 IEC 61508-1:1998 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 b)，因为该项只适合于 IEC 61508-1 的法文版。

d) 删除国际标准中 1.4 中的注，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。

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/TC124)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：冯晓升、王莉、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，所需的安全措施将依赖于应用中的具体因素。GB/T 20438 使这些措施规范化，以便将来引入到应用部门标准中。

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/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化目标失效量，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、技术和措施方法以达到 E/E/PE 安全相关系统的功能安全，但未使用失效-安全的概念，虽然这个概念在很好定义了失效模式和复杂性相对较低时可能非常有用。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1部分:一般要求

1　范围

1.1　GB/T 20438包含电气/电子/可编程电子系统在执行安全功能时要考虑的各个方面。GB/T 20438的一个主要目的是促进各应用领域的技术委员会制定应用领域的国家标准。这样将能充分考虑与应用有关的所有因素,因此可满足应用领域的需要。GB/T 20438的另一个目的是在没有应用领域国家标准的情况下能够开发电气/电子/可编程电子系统。

1.2　GB/T 20438尤其:

a)　适用于包含有一个或几个电气/电子/可编程电子装置的安全相关系统。

注1:对于简单的E/E/PE安全相关系统,GB/T 20438规定的有些要求是不必要的,可以不按这些要求(见4.2和GB/T 20438.4—2006的3.4.4中简单E/E/PE安全相关系统的定义)。

注2:尽管人也是安全相关系统的一部分(见GB/T 20438.4—2006的3.4.1),但GB/T 20438未细致考虑E/E/PE安全相关系统设计中人的因素。

b)　包含了E/E/PE安全相关系统所执行的安全功能失效引起的可能危险,这种可能危险应与E/E/PE设备本身产生的危险(如电击等)加以区分。

c)　不包括在如下情况时的E/E/PE系统:

——提供必要的风险降低能力的单一E/E/PE系统;并且

——E/E/PE系统安全完整性的要求低于规定的安全完整性等级1(GB/T 20438规定的最低安全完整性等级)。

d)　主要针对其失效将对人和/或环境安全产生影响的E/E/PE安全相关系统;但是,失效的后果也将对经济产生严重影响。从这个角度讲,GB/T 20438也涵盖了用于保护设备和产品的E/E/PE系统。

e)　考虑了E/E/PE安全相关系统、其他技术安全相关系统和外部风险降低设施,以便能系统地、以基于风险的方式确定E/E/PE安全相关系统的安全规范。

f)　用整体安全生命周期模型作为技术框架,系统地论述了为保证E/E/PE安全相关系统功能安全所需的活动。

注3:整体安全生命周期的初期阶段如需要还可包括其他技术安全相关系统和外部风险降低设施,以便能系统地、以基于风险的方式制定E/E/PE安全相关系统的要求规范。

注4:整体安全生命周期尽管是针对E/E/PE安全相关系统提出的,但同时也提供了一个考虑任何安全相关系统的技术框架,而不论这种安全相关系统使用何种技术(例如机械的、液压的或气动的)。

g)　不对各领域应用规定安全完整性等级(这要以领域应用的详细信息和知识为基础),这要由负责制定各应用领域标准的技术委员会在相应的标准中做出规定。

h)　对于尚无标准的各应用领域提供一个E/E/PE安全相关系统的通用要求。

i)　不包括防止未经批准人员对E/E/PE安全相关系统的损伤和/或对E/E/PE安全相关系统的安全功能产生不利影响的预防措施。

1.3　本部分是一般要求,它适用于GB/T 20438所有部分。GB/T 20438其他部分涉及更具体的问题:

——第2部分和第3部分对E/E/PE安全相关系统(硬件和软件)提出了更多的和具体的要求;

——第4部分规定GB/T 20438中使用的术语定义和缩略语;

——第5部分用举例的方法,对应用第1部分时如何确定安全完整性等级提供指南;

——第6部分给出了应用第2部分和第3部分的指南;

——第7部分包括技术和措施概述。