ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.1—2017/IEC 61508-1:2010
代替 GB/T 20438.1—2006

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 61508-1:2010,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

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1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 20438.1—2006《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》，与GB/T 20438.1—2006相比，主要技术变化如下：

——增加了功能安全管理中，人员能力的要求(见第6章)；

——增加了整体安全生命周期中，E/E/PE系统安全要求规范阶段(见7.10)；

——修改了评估独立性的评价方法(见第8章)。

本部分使用翻译法等同采用IEC 61508-1:2010《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》。

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、中国安全生产科学研究院、上海工业自动化仪表研究院、杭州和利时自动化有限公司、欧姆龙自动化(中国)有限公司、西门子(中国)有限公司、上海中沪电子有限公司。

本部分主要起草人：冯晓升、熊文泽、潘钢、史学玲、吴宗之、罗安、周有铮、杨柳、方来华、李佳嘉、李佳、郑威、张龙、王海清、孟邹清、梅豪。

本部分所代替标准的历次版本发布情况为：

——GB/T 20438.1—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。因而必须考虑各类安全策略，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，将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，建立一个足够健壮而广泛的能满足今后发展需要的框架；

——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宜具有高度一致性（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}；

——高要求运行模式或者连续运行模式下，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的主要目的是促进负责产品或应用领域的技术委员会制定产品和应用领域国家标准。这将允许充分考虑与产品或应用相关的所有因素,从而满足产品和应用领域用户的特定需要。GB/T 20438第二个目的是,在产品或应用领域没有国家标准的情况下能够开发E/E/PE安全相关系统。

1.2　GB/T 20438尤其:

a)　适用于包含有一个或几个电气/电子/可编程电子组件的安全相关系统;

注1:对于低复杂的E/E/PE安全相关系统,GB/T 20438规定的有些要求不是必要的,可以不符合(见4.2和GB/T 20438.4—2017的3.4.3中低复杂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—2017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有关人为因素的要求。

b)　是一个一般基础并适用于所有E/E/PE安全相关系统而无需考虑其具体应用;

c)　包括通过应用E/E/PE安全相关系统达到可容忍风险,但不包含E/E/PE设备自身出现的危险(如电击);

d)　可应用于所有类型的E/E/PE安全相关系统,包括保护系统和控制系统;

e)　不包括在下列情况时的E/E/PE系统:

——能够靠其自身能力满足可容忍风险的单一E/E/PE系统,并且

——该单一E/E/PE系统安全功能要求的安全完整性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)。

f)　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可用来规范任何用于保护设备和产品的E/E/PE系统;

注3:见GB/T 20438.4—2017的3.1.1。

g)　考虑了E/E/PE安全相关系统和其他风险降低措施,以便能系统性的、以基于风险的方式确定E/E/PE安全相关系统的安全要求规范;

h)　用整体安全生命周期模型作为技术框架,以便系统性地处理为确保E/E/PE安全相关系统功能安全所必需的活动;

注4:尽管整体安全生命周期首先是针对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)。

i)　不对各领域应用规定要求的安全完整性等级(这需要以该领域应用的详细信息和知识为基础),适合的安全完整性等级由负责制定各应用领域标准的技术委员会在行业应用标准中规定;

j)　对于尚无标准的各产品和应用领域提供E/E/PE安全相关系统的通用要求;

k)　需要在风险和危险分析时考虑恶意的和非授权的行为。分析范围包括所有相关的安全生命周期阶段;

注5:其他IEC/ISO标准对本条款有更详细的描写:参见ISO/IEC/TR 19791和IEC 62443系列标准。

l)　不包括防止未经批准人员损害E/E/PE安全相关系统的安全功能和/或对其产生不利影响的