

ICS 25.040
N 10



中华人民共和国国家标准

GB/T 20438.4—2006/IEC 61508-4:1998

GB/T 20438.4—2006/IEC 61508-4:1998

电气/电子/可编程电子安全相关系统的 功能安全 第4部分:定义和缩略语

Functional safety of electrical/electronic/programmable electronic
safety-related systems—Part 4: Definitions and abbreviations

(IEC 61508-4:1998, IDT)

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4部分:定义和缩略语
GB/T 20438.4—2006/IEC 61508-4:1998

*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045

网址 www.spc.net.cn
电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*
开本 880×1230 1/16 印张 1.5 字数 41 千字
2007年1月第一版 2007年1月第一次印刷

*
书号:155066·1-28710 定价 14.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究

举报电话:(010)68533533



GB/T 20438.4—2006

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	I
引言	II
1 范围	1
2 规范性引用文件	1
3 定义和缩略语	3
3.1 安全术语	3
3.2 设备和装置	4
3.3 系统:一般概念	5
3.4 系统:安全方面	7
3.5 安全功能和安全完整性	8
3.6 故障、失效和错误	10
3.7 生命周期活动	12
3.8 安全量的证实	13
参考文献	16
索引	17
图 1 GB/T 20438 的整体框架	2
图 2 可编程电子系统(PES):结构和术语	6
图 3 电气/电子/可编程电子系统(E/E/PES):结构和术语	6
图 4 失效模型	11
表 1 GB/T 20438 中使用的缩略语	3

测试装置(test harness)	3.8.15
允许风险(tolerable risk)	3.1.6
未检测到的(undetected)	3.8.9
未揭露的(unrevealed)	3.8.9
确认(validation)	3.8.2
验证(verification)	3.8.1

独立部门(independent department)	3.8.11
独立组织(independent organisation)	3.8.12
独立的人(independent person)	3.8.10
有限可变(limited variability)	3.2.7
逻辑系统(logic system)	3.4.5
简单 E/E/PE 安全相关系统(low-complexity E/E/PE safety-related system)	3.4.4
失误(mistake)	3.6.12
操作模式(mode of operation)	3.5.12
模块(module)	3.3.6
必要的风险降低(necessary risk reduction)	3.5.14
其他技术安全相关系统(other technology safety-related system)	3.4.2
明显的(overt)	3.8.8
可编程电子(programmable electronic)	3.2.5
可编程电子系统(PES)(programmable electronic system(PES))	3.3.2
检验测试(proof test)	3.8.5
随机硬件失效(Random hardware failure)	3.6.5
合理的可预见的误用(Reasonably foreseeable misuse)	3.1.11
冗余(redundancy)	3.3.10
揭露出的(revealed)	3.8.8
风险(risk)	3.1.5
安全失效(safe failure)	3.6.8
安全状态(safe state)	3.1.10
安全(safety)	3.1.8
安全功能(safety function)	3.5.1
安全功能要求规范(safety functions requirements specification)	3.5.9
安全完整性(safety integrity)	3.5.2
安全完整性等级(SIL)(safety integrity level(SIL))	3.5.6
安全完整性要求规范(safety integrity requirements specification)	3.5.10
安全生命周期(safety lifecycle)	3.7.1
安全软件(safety-related software)	3.5.11
安全相关系统(safety related system)	3.4.1
安全要求规范(safety requirements specification)	3.5.8
软件(software)	3.2.2
软件生命周期(software lifecycle)	3.7.2
软件模块(software module)	3.3.7
软件安全完整性(software safety integrity)	3.5.3
软件安全完整性等级(software safety integrity level)	3.5.7
系统(system)	3.3.1
系统失效(system failure)	3.6.6
系统安全完整性(systematic safety integrity)	3.5.4
目标失效量(target failure measure)	3.8.13

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 4 部分。

本部分等同采用国际标准 IEC 61508-4:1998《电气/电子/可编程电子安全相关系统的功能安全第 4 部分:定义和缩略语》(英文版)。

本部分与 IEC 61508-4:1998 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”。

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。