

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

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)

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1部分：一般要求  
GB/T 20438.1—2006/IEC 61508-1:1998

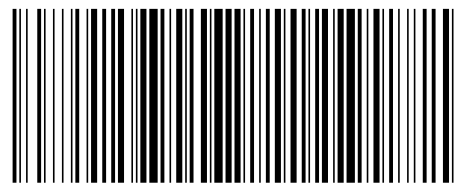
\*  
中国标准出版社出版发行  
北京复兴门外三里河北街16号  
邮政编码:100045

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 2.75 字数 77 千字  
2007年1月第一版 2007年1月第一次印刷

\*  
书号:155066·1-28708 定价 19.00 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 20438.1-2006

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 .....	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

## 参 考 文 献

- [1] IEC 60300-3-1:1991 可靠性管理 第 3 部分:应用指南 第 1 章:可靠性分析技术:方法论指南.
- [2] IEC 60300-3-9:1995 可靠性管理 第 3 部分:应用指南 第 9 章:技术系统的风险分析.
- [3] IEC 61355:1997 工厂、系统和设备文档的分类和命名.
- [4] IEC 61506:1997 工业过程测量和控制 应用软件文档.
- [5] ISO 8613-1:1994 信息技术 开放式文档体系结构(ODA)和交换格式:介绍和基本原理.
- [6] ISO 10007:1995 质量管理 配置管理指南.
- [7] ISO/IEC TR 15846 信息技术 软件生命周期过程 软件配置管理.
- [8] ANSI/ISA S84:1996 对过程工业装有安全仪表的系统的应用.
- [9] 在安全和可靠性研究中,处理共同原因失效的规程 规程框架和示例. NUREG/CR-4780, 1988-01,1.
- [10] 在安全和可靠性研究中,处理共同原因失效的规程 分析背景和技术. NUREG/CR-4780, 1989-01,2.