



中华人民共和国国家标准

GB/T 21109.1—2007/IEC 61511-1:2003

过程工业领域安全仪表系统的功能安全 第1部分：框架、定义、系统、硬件和 软件要求

Functional safety—Safety instrumented systems for the process
industry sector—Part 1: Framework, definitions, system,
hardware and software requirements

(IEC 61511-1:2003, IDT)

2007-10-11 发布

2007-12-01 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	V
引言	VI
1 范围	1
2 规范性引用文件	4
3 缩略语和定义	4
3.1 缩略语	4
3.2 术语和定义	5
4 与 GB/T 21109 的符合性	18
5 功能安全管理	18
5.1 目的	18
5.2 要求	18
6 安全生命周期要求	21
6.1 目的	21
6.2 要求	21
7 验证	23
7.1 目的	23
8 过程危险和风险评估	23
8.1 目的	23
8.2 要求	24
9 给保护层分配安全功能	24
9.1 目的	24
9.2 分配过程要求	24
9.3 安全完整性等级 4 的附加要求	25
9.4 对作为一个保护层的基本过程控制系统的要求	25
9.5 防止共同原因失效、共同模式失效和相关失效的要求	26
10 SIS 安全要求规范	26
10.1 目的	26
10.2 一般要求	26
10.3 SIS 安全要求	27
11 SIS 设计和工程	27
11.1 目的	27
11.2 一般要求	28
11.3 检测故障时的系统行为要求	28
11.4 硬件故障裕度要求	29
11.5 选择部件和子系统的要求	30
11.6 现场装置	32
11.7 接口	33
11.8 维护或测试设计要求	34

11.9	SIF 的失效概率	34
12	应用软件要求,包括工具软件的选择准则	35
12.1	应用软件安全生命周期要求	36
12.2	应用软件安全要求规范	40
12.3	应用软件安全确认计划编制	41
12.4	应用软件设计和开发	42
12.5	应用软件与 SIS 子系统的集成	45
12.6	FPL 和 LVL 软件修改规程	46
12.7	应用软件验证	46
13	工厂验收测试(FAT)	47
13.1	目的	47
13.2	建议	47
14	SIS 安装和调试运行	48
14.1	目的	48
14.2	要求	48
15	SIS 安全确认	49
15.1	目的	49
15.2	要求	49
16	SIS 操作和维护	51
16.1	目的	51
16.2	要求	51
16.3	检验测试和检查	52
17	SIS 修改	53
17.1	目的	53
17.2	要求	53
18	SIS 停用	53
18.1	目的	53
18.2	要求	53
19	信息和文档要求	54
19.1	目的	54
19.2	要求	54
	附录 A (资料性附录) 差异	55
	参考文献	56
图 1	GB/T 21109 的整体框架	VI
图 2	GB/T 21109 与 GB/T 20438—2006 的关系	2
图 3	GB/T 21109 与 GB/T 20438—2006 的关系(见第 1 章)	2
图 4	仪表安全功能和其他功能的关系	3
图 5	本部分的系统、硬件和软件的关系	3
图 6	可编程电子系统(PES):结构和术语	12
图 7	SIS 结构示例	14
图 8	SIS 安全生命周期阶段和功能安全评估阶段	20
图 9	过程工厂中常见的典型风险降低方法	26

图 10	应用软件安全生命周期及其与 SIS 安全生命周期的关系	36
图 11	应用软件安全生命周期(在实现阶段)	37
图 12	软件开发生命周期(V 模型)	38
图 13	SIS 硬件和软件结构之间的关系	40
表 1	GB/T 21109 中使用的缩略语	4
表 2	SIS 安全生命周期一览表	22
表 3	安全完整性等级:要求时的失效概率	25
表 4	安全完整性等级:SIF 的危险失效频率	25
表 5	PE 逻辑解算器的最低硬件故障裕度	30
表 6	传感器、最终元件和非 PE 逻辑解算器的最低硬件故障裕度	30
表 7	应用软件安全生命周期一览表	38
表 A.1	组织上的差异	55
表 A.2	术语上的差异	55

前 言

GB/T 21109《过程工业领域安全仪表系统的功能安全》分为三个部分：

- 第1部分：框架、定义、系统、硬件和软件要求；
- 第2部分：GB/T 21109.1的应用指南；
- 第3部分：确定要求的安全完整性等级的指南。

本部分为GB/T 21109的第1部分，等同采用IEC 61511-1:2003《过程工业领域安全仪表系统的功能安全 第1部分：框架、定义、系统、硬件和软件要求》(英文版)。为便于使用，对IEC 61511-1:2003做了下列编辑性修改：

- 删除国际标准的前言，按GB/T 1.1—2000重新编写了本部分的前言；
- 凡是出现“IEC 61511”之处均改为“GB/T 21109”，“IEC 61511-1”均改为“GB/T 21109.1”，“IEC 61511-2”均改为“GB/T 21109.2”，“IEC 61511-3”均改为“GB/T 21109.3”；
- 凡是出现“本国际标准”之处均改为“GB/T 21109”；
- 用小数点“.”代替作小数点的逗号“,”；
- 根据GB/T 1.1—2000进行编辑性修改。

本部分的附录A为资料性附录。

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归口。

本部分主要起草单位：机械工业仪器仪表综合技术经济研究所、上海自动化仪表股份有限公司技术中心、北京华控技术有限责任公司、中科院沈阳自动化研究所、浙江中控技术有限公司、上海工业自动化仪表研究所、国营759厂。

本部分主要起草人：王春喜、梅恪、包伟华、王麟琨、刘丹、陈小枫、魏剑崑、史学玲、谭平、李佳嘉、欧阳劲松、蔡廷安、马光武。

本部分为首次制定。