ICS 25.040
N 10

中华人民共和国国家标准

GB/T 21109.2—2007/IEC 61511-2:2003

过程工业领域安全仪表系统的功能安全 第2部分:GB/T 21109.1的应用指南

Functional safety—Safety instrumented systems for the process industry sector—Part 2:Guidelines for the application of GB/T 21109.1

(IEC 61511-2:2003,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

GB/T 21109.2—2007/IEC 61511-2:2003

中华人民共和国
国家标准
过程工业领域安全仪表系统的功能安全
第2部分:GB/T 21109.1的应用指南
GB/T 21109.2—2007/IEC 61511-2:2003
*
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 3.75　字数 101 千字
2008年1月第一版　2008年1月第一次印刷
*
书号:155066·1-30412　定价 38.00 元

GB/T 21109.2-2007

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和缩略语 …… 1
4　与GB/T 21109的符合性 …… 1
5　功能安全管理 …… 1
5.1　目的 …… 1
5.2　要求 …… 1
6　安全生命周期要求 …… 6
6.1　目的 …… 6
6.2　要求 …… 6
7　验证 …… 6
7.1　目的 …… 6
8　过程危险和风险评估 …… 7
8.1　目的 …… 7
8.2　要求 …… 7
9　给保护层分配安全功能 …… 9
9.1　目的 …… 9
9.2　分配过程的要求 …… 9
9.3　安全完整性等级4的附加要求 …… 10
9.4　作为一个保护层的基本过程控制系统的要求 …… 10
9.5　防止共同原因失效、共同模式失效和相关失效的要求 …… 11
10　SIS安全要求规范 …… 12
10.1　目的 …… 12
10.2　一般要求 …… 12
10.3　SIS安全要求 …… 12
11　SIS设计和工程 …… 13
11.1　目的 …… 13
11.2　一般要求 …… 13
11.3　检测故障时的系统行为要求 …… 16
11.4　硬件故障裕度要求 …… 16
11.5　选择部件和子系统的要求 …… 17
11.6　现场装置 …… 18
11.7　接口 …… 19
11.8　维护或测试设计要求 …… 20
11.9　SIF的失效概率 …… 21
12　应用软件要求，包括工具软件的选择准则 …… 22

12.1 应用软件安全生命周期要求 …… 22
12.2 应用软件安全要求规范 …… 25
12.3 应用软件安全确认计划编制 …… 26
12.4 应用软件设计和开发 …… 26
12.5 应用软件与 SIS 子系统的集成 …… 31
12.6 FPL 和 LVL 软件修改规程 …… 31
12.7 应用软件验证 …… 32
13 工厂验收测试(FAT) …… 33
13.1 目的 …… 33
13.2 建议 …… 33
14 SIS 安装和调试运行 …… 33
14.1 目的 …… 33
14.2 要求 …… 33
15 SIS 安全确认 …… 33
15.1 目的 …… 33
15.2 要求 …… 33
16 SIS 操作和维护 …… 34
16.1 目的 …… 34
16.2 要求 …… 34
16.3 检验测试和检查 …… 34
17 SIS 修改 …… 35
17.1 目的 …… 35
17.2 要求 …… 35
18 SIS 停用 …… 35
18.1 目的 …… 35
18.2 要求 …… 35
19 信息和文档要求 …… 36
19.1 目的 …… 36
19.2 要求 …… 36
附录 A(资料性附录) 计算一个仪表安全功能要求时的失效概率的技术示例 …… 37
附录 B(资料性附录) 典型的 SIS 结构开发 …… 38
附录 C(资料性附录) 安全 PLC 的应用特征 …… 42
附录 D(资料性附录) SIS 逻辑解算器应用软件开发方法的示例 …… 44
附录 E(资料性附录) 开发安全配置的 PE 逻辑解算器的外配诊断程序的示例 …… 48

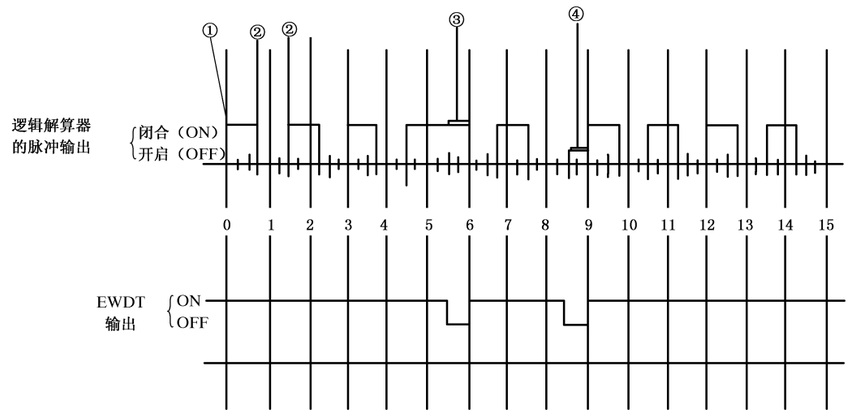
图 1 GB/T 21109 的整体框架 …… Ⅴ
图 2 BPCS 功能和诱发原因的独立性说明 …… 11
图 3 软件开发生命周期(V 模型) …… 23
图 B.1 实现 SIL 使用的模型 …… 39
图 C.1 逻辑解算器 …… 42
图 E.1 EWDT 定时图 …… 49
表 1 典型的安全手册编排方式和内容 …… 30
表 B.1 典型的 SIS 生命周期步骤 …… 38

按钮。当设计复位电路时,EWDT 和 IWDT 两者都应被考虑。

- 可能需要的测试按钮。为验证 EWDT 的功能性可能需要一个测试按钮。
- 专用 PE 逻辑解算器的输出被用来监视逻辑解算器输出总线状态以便检测异常运行。
- 减少机电继电器触点产生的对电子电路的感应干扰的浪涌抑制器。应复审满足规定要求的附加电源线路的应用,比如:欠压保护,电噪声抑制,闪电保护,报警设计,从而能确定是 EWDT 启动或是 IWDT 启动。

E.3 参考

CCPS, "Guidelines for Safe Automation of Chemical Processes", AIChE, 345 East 47th Street, New York, New York 10017, ISBN 0-8169-0554-1, 1993。



① 闭合控制电路给输出加电。
② 在定时间隔(假设定为 1 s)结束之前,开启和闭合控制电路以保持给 EWDT 输出加电。只要被监视的脉动持续提供每个定时间隔至少 1 次转换,该输出就保持加电。
③ 如果被监视的控制的闭合(ON)的持续时间大于预设时间(③),EWDT 的输出就会被断电。
④ 如果被监视的控制的开启(OFF)的持续时间大于预设时间(④),EWDT 的输出也会被断电。

图 E.1 EWDT 定时图