

Safety Instrumented Systems:
Design, Analysis and Justification,
2nd Edition

安全仪表系统 工程设计与应用

(第二版)

[美] Paul Gruhn, P.E.,CFSE Harry L. Cheddie ,P.Eng.,CFSE 编著
张建国 李玉明 译



中国石化出版社

[HTTP://WWW.SINOPEC-PRESS.COM](http://www.sinopec-press.com)

安全仪表系统 工程设计与应用

(第二版)

**Safety Instrumented Systems: Design,
Analysis and Justification, 2nd Edition**

[美] Paul Gruhn, P. E., CFSE 编著
Harry L. Cheddie, P. Eng., CFSE
张建国 李玉明 译

中国石化出版社

内 容 提 要

本书从实际工程应用出发,阐述了对 SIS 应用如何进行分析、设计、工程集成、安装,以及操作和维护。

本书面向过程工业领域仪表和控制系统工程师,特别适合从事安全仪表系统(SIS)设计、安装,以及维护工作的读者参考。在最终用户、工程公司、系统集成商,以及咨询服务机构中与 SIS 应用相关的工程技术人员、项目经理,以及销售人员,都可以从本书受益。

著作权合同登记 图字:01-2016-5800 号

Safety Instrumented Systems: Design, Analysis and Justification, 2nd Edition By Paul Gruhn, P. E., CFSE and Harry L. Cheddie, P. Eng., CFSE.

ISBN: 1-55617-956-1

“Copyright © 2006 ISA. All rights reserved. Reprinted in limited copies with permission. Photocopies are prohibited under international copyright laws.

版权 2006 ISA. 版权所有。许可限量再次印刷。国际版权法禁止影印。”

版权© 2006 由 ISA—仪表、系统和自动化学会; 亚历山大大道 67 号 (67 Alexander Drive); 邮政信箱: 12277 (P. O. Box 12277); 三角地研究园, NC 27709 (Research Triangle Park, NC 27709) 版权所有。

未经出版商书面许可,不得将本书的任何内容复制存储于检索系统,或者以电子、机械、影印、录音或者其他等任何手段以任何形式传播。

中文版权为中国石化出版社所有。版权所有,不得翻印。

图书在版编目(CIP)数据

安全仪表系统工程设计与应用 / (美) 保罗格润,
(美) 哈瑞·L. 谢迪编著; 张建国, 李玉明译. —2 版.
—北京: 中国石化出版社, 2017. 5

书名原文: Safety Instrumented Systems: Design,
Analysis and Justification, 2nd Edition

ISBN 978-7-5114-4408-0

I. ①安… II. ①保… ②哈… ③张… ④李… III. ①安全
仪表-设计 IV. ①TH89

中国版本图书馆 CIP 数据核字(2017)第 099482 号

未经本社书面授权,本书任何部分不得被复制、抄袭,或者以任何形式或任何方式传播。版权所有,侵权必究。

中国石化出版社出版发行

地址:北京市朝阳区吉市口路 8 号

邮编:100020 电话:(010)59964500

发行部电话:(010)59964526

http://www.sinopec-press.com

E-mail: press@sinopec.com

北京科信印刷有限公司印刷

*

700×1000 毫米 16 开本 17 印张 311 千字

2017 年 5 月第 2 版 2017 年 5 月第 1 次印刷

定价:98.00 元



通 告

本出版物中的所有资料，用于读者的普通教育。由于作者和出版商没有任何控制能力约束读者对这些资料的使用，因此作者和出版商双方都拒绝承担因读者使用这些内容引发的任何类型的部分以及全部责任。期望读者在将本书的任何内容用于特定应用时，应自行作出全面的专业评判。

此外，作者和出版商没有调查和考虑在将书中的任何资料用于特定应用时，读者的能力对任何专利的影响。读者有责任审查任何可能的专利对将本书资料用于任何特定应用时有可能造成限制。

本书中提及的任何市面上的实物产品，都仅仅是作为例子引用。作者和出版商不会对引用的任何实物产品背书。引用的任何商标或者商品名称属于各自的拥有者。作者和出版商在任何时候都不对引用的任何实物产品的有效性作出表示。在使用实物产品时，在任何时候都应遵循制造商的说明书，即使与本书中给出的资料相矛盾。

译者致谢

翻译这本书的动议，来自于国家安全生产监督管理总局安监总管三〔2014〕116号“国家安全监管总局关于加强化工安全仪表系统管理的指导意见”的实施。

该指导意见明确要求加快安全仪表系统功能安全相关技术和管理人才的培养要通过开展安全仪表专业培训，强化功能安全相关知识，培养一批具备专业技术能力、掌握相关标准规范的工程技术人员，满足开展和加强化工安全仪表系统功能安全管理工作的需要。这本书的翻译旨在为广大业界读者提供一份可供参考的资料。

随着现代过程工业生产规模的日益庞大，复杂的工艺技术和生产装备的广泛采用，生产装置和设施的“过程安全”成为重要的课题。采用仪表和自动控制技术的紧急停车系统、安全关断系统，以及安全连锁系统等名目繁多的安全保护系统为确保安全生产功不可没，同时由于这些系统本身的故障或功能失效导致意外事故发生也屡见不鲜。经过几十年的仪表技术和安全生产理论的发展进步，推动了 IEC 61508/IEC 61511 等“功能安全”国际标准的制定。这些标准规范的显著特点，是以“性能化”设计和全生命周期管理为导向，以安全完整性等级 (SIL) 为指针，为形形色色的仪表保护系统应用确立了统一的设计和工程实践准则。

基于 IEC 61508 的国家标准 GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》和基于 IEC 61511 的国家标准 GB/T 21109《过程工业领域安全仪表系统的功能安全》颁布十余年来，受到政府安全监管部门和业界的重视和认可。但是，市面上有关安全仪表系统工程应用的书籍并不多见。本书的翻译出版，在一定程度上对读者了解安全仪表的相关概念和技术应用会有所帮助。

本书的原著，是美国 ISA (International Society of Automation) 出版的《Safety Instrumented Systems: Design, Analysis and Justification, 2nd Edition》。该书是美国 ISA 84 安全仪表系统认证程序 (ISA 84 Safety

Instrumented Systems Certificate Programs) 1 级证书-SIS 基础技术专员 (Certificate 1: ISA 84 SIS Fundamentals Specialist) 的培训教材 (ISA 培训课程编号 EC 50)。由于是 SIS 的基础知识培训教材, 本书作者在行文上尽量避免采用专业术语和定义, 而是用生动的语言、形象的比喻解释有关 SIS 应用的相关概念和知识, 特别适合于初级学习之用。

这本书中介绍的法律法规以及 SIS 工程应用的技术背景立足于美国, 很多方面并不适用于我国的安全监管和工程实践要求。不过, 基于我国企业开拓国际市场以及学习欧美发达国家的先进技术和安全理念的现实需要, 广大读者一定会从本书受益。

本书的原作者是保罗格润 (Paul Gruhn, P. E., CFSE) 和哈瑞 L. 谢迪 (Harry L. Cheddie, P. Eng., CFSE)。在本书翻译出版之际, 译者对原作者表达敬意和感谢。

原著对这两位作者的介绍如下:

保罗格润是位于得克萨斯州休斯顿市的 ICS Triplex 公司的安全专家。保罗是 ISA 会员和 ISA SP84 委员会成员。ISA SP84 委员会编写了 ISA 84 系列标准—1996 版“安全仪表系统在过程工业中的应用”和 2004 版“过程工业安全仪表系统的功能安全”。保罗是 ISA 课程 EC 50—“安全仪表系统”课件的编者和讲师。保罗积极参与 ISA 在当地或国家层面的各种活动。保罗也是系统安全学会 (System Safety Society) 和国家专业工程师学会 (National Society of Professional Engineers) 的成员。保罗拥有伊利诺伊州芝加哥市伊利诺伊技术学院的机械工程学士学位, 是得克萨斯州执业专业工程师, TÜV 认证的功能安全专家。

哈瑞 L. 谢迪是 Exida 的首席工程师和合伙人。目前从事安全技术研究工作, 并基于 IEC 61508 和 IEC 61511 标准开展培训课程开发以及教学。加入 Exida 之前, 哈瑞是位于加拿大安大略萨尼亚市的拜耳公司的控制系统顾问, 同时也是工程部门的主管, 负责过程控制系统的设计和维修。哈瑞毕业于英国索尔福德大学, 电气工程学士 (优等荣誉) 学位。加拿大安大略省注册专业工程师。哈瑞是美国质量学会 (American Society for Quality) 认证的质量工程师和可靠性工程师, TÜV 认证的功能安全专家。

本书的翻译出版，得到了国家安监总局领导的直接关怀、支持和鼓励，得到各级安监部门和团体相关领导以及业界各方朋友的支持和大力协助，得到中国石化出版社的热忱合作，以及得到 ISA 的信任和肯定，得到译者工作单位领导的大力支持和同事们热情帮助。译者对各级领导和各方朋友对本书出版给予的支持和帮助表示深深的谢忱和敬意。

还要特别感谢下列团体对本书出版发行给予的大力支持：

- 中国化学品安全协会
- 中国自动化学会仪表与装置专业委员会
- 中国化工学会培训中心
- 中国石油和化学工业联合会(上海)培训中心
- 广东新华粤华德科技有限公司
- 北京安稳优自动化技术有限公司

本书中相关概念的翻译既参照国标，也考虑了石化和化工行业的通行表达，在行文上尽量保持原著的风格，也修正了一些明显错误。不过由于译者的水平所限，表达不准确或者可能出现差错很难完全避免。诚恳地欢迎广大读者朋友批评指正。

译者

目 录

1 概述	(1)
1.1 安全仪表系统	(2)
1.2 本书服务对象	(3)
1.3 本书意图	(3)
1.4 业界的困惑	(4)
1.4.1 技术选择	(5)
1.4.2 冗余选择	(5)
1.4.3 现场仪表	(5)
1.4.4 测试周期	(5)
1.4.5 厂商宣传	(6)
1.4.6 认证与早先使用	(6)
1.5 工业指南、标准以及法规	(6)
1.5.1 HSE-PES	(7)
1.5.2 AIChE-CCPS	(7)
1.5.3 IEC 61508	(7)
1.5.4 ANSI/ISA-84.00.01—2004(IEC 61511 Mod)和 ANSI/ISA-84.01—1996	(8)
1.5.5 NFPA 85	(8)
1.5.6 API RP 556	(9)
1.5.7 API RP 14C	(9)
1.5.8 OSHA(29 CFR 1910.119-高危险化学品的过程安全管理)	(9)
1.6 标准制定思路的变化	(11)
1.7 不能仅凭感觉	(12)
1.8 自满是危险的	(13)
1.9 学习永无止境	(14)
小结	(14)
参考文献	(15)
2 安全生命周期	(16)
2.1 后知后觉与先知先觉	(17)



2.2	HSE 的调查结果	(18)
2.3	安全生命周期	(20)
2.3.1	危险和风险分析	(21)
2.3.2	将安全功能分配到保护层	(21)
2.3.3	编制安全要求规格书	(22)
2.3.4	SIS 设计和工程	(22)
2.3.5	安装、调试及确认	(23)
2.3.6	操作和维护	(23)
2.3.7	修改	(24)
2.3.8	停用	(24)
	小结	(24)
	参考文献	(24)
3	过程控制与安全控制	(26)
3.1	控制和安全定义	(27)
3.2	过程控制的特征——主动的或动态的	(28)
3.2.1	需要频繁更改控制方式	(28)
3.3	安全控制的特征——被动的或休眠的	(29)
3.3.1	需要限制更改	(30)
3.3.2	要求模式与连续模式	(30)
3.4	控制系统和安全系统分别设置	(30)
3.4.1	HSE-PES	(31)
3.4.2	AICHe-CCPS	(31)
3.4.3	IEC 61508	(32)
3.4.4	ANSI/ISA-84.00.01—2004	(32)
3.4.5	API RP 14C	(33)
3.4.6	API RP 554	(34)
3.4.7	NFPA 85	(34)
3.4.8	IEEE 603	(34)
3.5	共因失效与系统或功能失效	(35)
3.5.1	人力因素	(36)
	小结	(37)
	参考文献	(37)
4	保护层	(39)
4.1	预防保护层	(42)



4.1.1	工艺装置设计	(42)
4.1.2	过程控制系统	(43)
4.1.3	报警系统	(43)
4.1.4	操作规程	(44)
4.1.5	停车、联锁仪表系统(安全仪表系统——SIS)	(45)
4.1.6	物理保护措施	(45)
4.2	减轻保护层	(45)
4.2.1	封闭系统	(45)
4.2.2	洗涤设备和火炬	(46)
4.2.3	火气(F&G)系统	(46)
4.2.4	紧急疏散程序	(47)
4.3	差异化措施	(47)
	小结	(48)
	参考文献	(49)
5	编制安全要求规格书	(50)
5.1	概述	(51)
5.2	44%的事故归咎于不正确的技术要求规格书	(51)
5.2.1	管理系统	(52)
5.2.2	工作程序	(53)
5.2.3	评估的时间安排	(53)
5.2.4	核心人员参与审查过程	(54)
5.2.5	职责不明	(54)
5.2.6	培训和工具	(54)
5.2.7	复杂性和不切实际的预期	(54)
5.2.8	文档不完整	(55)
5.2.9	规格书最终审查不到位	(57)
5.2.10	规格书中存在未被认可的背离	(57)
5.3	ANSI/ISA-84.00.01—2004(IEC 61511 Mod)第1~3部分的要求	(57)
5.4	规格书文档要求	(59)
	小结	(59)
	参考文献	(60)
6	确定安全完整性等级(SIL)	(61)
6.1	概述	(62)
6.2	责任主体	(63)



6.3	技术方法	(63)
6.4	共性问题	(64)
6.5	评估风险	(64)
6.5.1	危险	(64)
6.5.2	风险	(65)
6.5.3	致死率	(65)
6.5.4	现代社会的内在风险	(66)
6.5.5	自愿风险与非自愿风险	(67)
6.5.6	可容忍风险	(68)
6.5.7	过程工业可容忍风险	(68)
6.6	安全完整性等级	(70)
6.7	SIL 定级方法 1——合理尽可能低的原则(ALARP)	(71)
6.8	SIL 定级方法 2——风险矩阵	(72)
6.8.1	评估频率	(73)
6.8.2	评估严重性	(73)
6.8.3	评估整体风险	(74)
6.8.4	附加保护层的有效性	(74)
6.9	SIL 定级方法 3——风险图	(76)
6.10	SIL 定级方法 4: 保护层分析(LOPA)	(77)
6.10.1	可容忍的风险	(78)
6.10.2	触发事件频率	(79)
6.10.3	安全保护层的安全性能水平	(79)
6.10.4	LOPA 举例	(80)
	小结	(83)
	参考文献	(83)
	其他资料	(84)
7	选择技术	(85)
7.1	气动系统	(86)
7.2	继电器系统	(86)
7.3	固态系统	(88)
7.4	微处理器、PLC(基于软件的)系统	(89)
7.4.1	灵活性优缺点	(90)
7.4.2	软件问题	(90)
7.4.3	通用 PLC	(91)



7.4.4 安全 PLC	(94)
7.5 与系统规模有关的问题	(97)
7.6 与系统复杂性有关的问题	(98)
7.7 与其他系统之间的通信	(98)
7.8 认证与早先使用	(99)
小结	(100)
参考文献	(101)
8 系统评估	(102)
8.1 透过现象看本质	(103)
8.2 前期分析的重要性	(105)
8.2.1 事先警告	(105)
8.3 怎样获取失效率信息?	(106)
8.3.1 维护记录	(107)
8.3.2 供货商记录	(107)
8.3.3 第三方数据库	(107)
8.3.4 军用形式的计算	(108)
8.4 失效模式	(108)
8.4.1 安全失效、危险失效	(109)
8.4.2 检测出的失效、未被检测出的失效	(110)
8.5 测量尺度	(110)
8.5.1 失效率、MTBF 以及生命期	(112)
8.6 建模的精确程度	(113)
8.7 建模方法	(114)
8.7.1 可靠性方块图	(114)
8.7.2 故障树	(115)
8.7.3 马尔可夫模型	(116)
8.8 冗余的影响	(116)
8.9 基本公式	(119)
8.9.1 人工测试持续时间的影响	(120)
8.10 继电器系统分析	(121)
8.11 非冗余 PLC 系统分析	(121)
8.12 TMR 系统分析	(122)
8.12.1 公共原因	(123)
8.13 现场仪表	(125)



8.13.1 阀门的部分行程测试	(126)
8.14 故障容错要求	(128)
8.15 SIS 设计样本	(129)
8.16 分析系统性能的工程工具	(130)
小结	(130)
参考文献	(131)
9 与现场仪表有关的问题	(133)
9.1 概述	(134)
9.2 现场仪表的重要性	(134)
9.2.1 现场仪表对系统性能的影响	(134)
9.2.2 系统失效各部分比例	(135)
9.3 传感器	(136)
9.3.1 概述	(136)
9.3.2 检测开关	(138)
9.3.3 变送器	(139)
9.3.4 传感器的失效诊断	(140)
9.3.5 智能变送器	(141)
9.4 最终元件	(141)
9.4.1 概述	(142)
9.4.2 阀门的失效诊断	(143)
9.4.3 智能阀门定位器	(143)
9.5 冗余	(144)
9.5.1 表决配置和冗余	(145)
9.6 现场仪表设计要求	(147)
9.6.1 传感器设计要求	(148)
9.6.2 最终元件设计要求	(149)
9.7 安装关注点	(151)
9.8 现场仪表接线	(151)
小结	(152)
参考文献	(152)
10 安全系统的工程实施	(153)
10.1 管理要求	(154)
10.1.1 时间安排和工作内容定义	(154)
10.1.2 人员	(154)



10.1.3	沟通	(155)
10.1.4	文档	(155)
10.2	硬件设计考虑	(155)
10.2.1	得电关停与失电关停系统	(155)
10.2.2	系统诊断	(156)
10.2.3	共因的最小化	(157)
10.2.4	盘柜设计	(157)
10.2.5	环境因素	(158)
10.2.6	供电	(158)
10.2.7	接地	(159)
10.2.8	检测开关和继电器的选择	(159)
10.2.9	旁路	(159)
10.2.10	功能测试	(160)
10.2.11	安保措施	(160)
10.2.12	操作员接口	(161)
10.3	软件设计考虑	(162)
10.3.1	软件的生命周期	(162)
10.3.2	程序和编程语言类型	(164)
10.3.3	软件性能的量化	(165)
10.3.4	软件测试	(166)
	小结	(167)
	参考文献	(167)
11	安全系统的安装	(168)
11.1	概述	(169)
11.2	术语	(170)
11.3	工厂验收测试(FAT)	(171)
11.4	安装	(172)
11.4.1	安装检查	(173)
11.5	确认、现场验收测试(SAT)	(174)
11.5.1	必要的文档	(175)
11.6	功能安全评估、开车前安全审查(PSSR)	(175)
11.7	培训	(176)
11.8	交付给工艺操作部门	(177)
11.9	开车	(177)



11.10	开车之后的后续活动	(178)
	小结	(178)
	参考文献	(179)
12	功能测试	(180)
12.1	概述	(181)
12.2	测试的需要	(181)
12.2.1	ANSI/ISA-84.00.01—2004 对功能测试的要求	(184)
12.2.2	一般性指南	(185)
12.3	确定测试频率	(186)
12.4	测试的责任主体	(187)
12.5	测试装备和规程	(187)
12.6	文档	(189)
12.6.1	测试规程文档样本	(190)
	小结	(192)
	参考文献	(192)
13	系统的变更管理	(193)
13.1	概述	(194)
13.2	变更管理的需要	(194)
13.3	何时要求变更管理(MOC)?	(195)
13.4	何时不适用变更管理?	(196)
13.5	ANSI/ISA-84.00.01—2004 的要求	(197)
13.6	变更管理(MOC)规程	(199)
13.7	变更管理(MOC)文档	(200)
	小结	(201)
	参考文献	(201)
14	安全系统的可行性评判	(202)
14.1	概述	(203)
14.2	安全系统失效模式	(204)
14.3	可行性评判	(206)
14.4	评判的责任主体	(207)
14.5	如何进行评判	(207)
14.6	生命周期成本	(209)
14.7	审查示例	(210)
14.8	生命周期成本分析	(214)



14.9 优化安全、可靠性以及生命周期成本.....	(216)
小结	(217)
参考文献	(217)
15 SIS 设计检查表	(218)
15.1 概述.....	(219)
15.2 检查表概览.....	(220)
第1部分: 管理要求	(221)
第2部分: 安全要求规格书	(222)
第3部分: SIS 的概念设计	(223)
第4部分: SIS 的详细设计	(224)
第5部分: 供电和接地	(225)
第6部分: 现场仪表	(226)
第7部分: 操作员接口	(227)
第8部分: 维护和工程接口	(228)
第9部分: 通信	(228)
第10部分: 硬件技术规格书	(229)
第11部分: 硬件制造	(230)
第12部分: 应用逻辑要求	(230)
第13部分: 嵌入(厂商)软件	(231)
第14部分: 软件组态	(232)
第15部分: 工厂测试	(233)
第16部分: 安装和调试	(234)
第17部分: 操作和维护	(236)
第18部分: 测试	(237)
第19部分: 变更管理	(238)
第20部分: 停用	(239)
参考文献	(239)
16 案例分析.....	(240)
16.1 概述.....	(241)
16.2 安全生命周期及其重要性.....	(241)
16.3 案例描述: 加热炉、燃烧加热器安全停车系统.....	(243)
16.4 分析范围.....	(244)
16.5 确定 SIL 目标值	(245)
16.6 制定安全要求规格书(SRS)	(246)



16.7	SIS 概念设计	(249)
16.8	生命周期成本分析.....	(251)
16.9	验证概念设计满足 SIL 要求	(252)
16.10	详细设计	(253)
16.11	安装、调试, 以及开车前测试	(254)
16.12	操作和维护规程	(254)
	小结	(256)
	参考文献	(256)