# 功能安全技术基础

刘建侯　主编

GONG NENG AN QUAN JI SHU JI CHU

机械工业出版社
CHINA MACHINE PRESS

# 功能安全技术基础

主编　刘建侯
参编　李佳嘉　谢亚莲　张艾森

机械工业出版社

本书以电气/电子/可编程电子（E/E/PE）安全相关系统为基础，对电子、机械以及特殊危险环境应用的安全相关装置及其系统功能安全的相关理论、方法和技术进行了详细介绍。在叙述可靠性技术和环境试验技术的基础上，以E/E/PE安全相关（控制）系统安全生命周期实现阶段中的各阶段为主线，对被控对象的风险评估以及E/E/PE安全相关系统的设计、分配、安全完整性等级（SIL）的估算、操作、维护、测试、确认和评估等各阶段展开了讨论。

本书内容丰富，深入浅出，案例清晰，在讲述功能安全技术基本方法的同时，注重与工程实际应用的结合。希望本书能为我国功能安全技术的推广和发展起到积极作用。

本书可供从事设备及自控系统设计、安装、制造、应用的工程技术人员和广大用户参考，也可作为大专院校及工程技术人员的培训教材。

**图书在版编目（CIP）数据**

功能安全技术基础/刘建侯主编. —北京：机械工业出版社，2008.5
ISBN 978-7-111-24042-6

Ⅰ.功… Ⅱ.刘… Ⅲ.安全技术 Ⅳ.X93

中国版本图书馆CIP数据核字（2008）第061099号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）
责任编辑：张沪光 版式设计：霍永明 责任校对：张玉琴
封面设计：陈 沛 责任印制：杨 曦
三河市国英印务有限公司印刷
2008年6月第1版第1次印刷
140mm×203mm·11印张·294千字
0001—5000册
标准书号：ISBN 978-7-111-24042-6
定价：25.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
销售服务热线电话：（010）68326294
购书热线电话：（010）88379639 88379641 88379643
编辑热线电话：（010）88379767
封面无防伪标均为盗版

# 前　言

电气/电子/可编程电子和控制设备是国民经济各部门重要的现代技术装备，被广泛用于冶金、电力、石油、化工、航空航天、机械、矿产、医药、交通、食品、农业、环保以及日常生活等各个领域。随着科学技术的发展，高新技术正在不断地扩展，由于大型复杂的现代化企业和现代化设备的建设，对产品质量的不断追求，要求产品不仅能在正常条件下工作，还要能在各种不同环境条件（如恶劣气候、振动、电磁骚扰等）下也要安全、可靠地工作。因而，对生产过程和制造过程中的功能安全要求也越来越高，为了减少各种风险，保证生产过程和制造过程的安全，人们采用了各种保护装置和安全系统，使电气/电子/可编程电子设备安全相关（控制）系统的应用范围越来越广泛。同时，对其自身的功能安全问题也已受到人们的广泛关注。所以，功能安全越来越受到人们的重视。

近十几年来，国内电子、机械、仪表、船舶、冶金、航空航天、邮电、电力、建筑和军工等行业都引进了许多国外设备，同时也引进了国外的技术（包括技术标准、性能要求及试验方法等）。我们一方面通过消化吸收、批量生产和新产品的研制开发等实践，逐步地掌握了国外的先进工艺，严格的试验方法和先进的管理方法，从而推动了国产设备质量的提高，为国产设备立足国内市场，开拓国外市场打下了良好的基础；另一方面通过对国外引进产品和国内企业（包括合资企业）产品的质量评估，使用户获得可靠、安全放心的产品。

目前，国外在功能安全技术方面已经进行了大量的研究，目的是保障安全系统在必要时能正确有效地执行其安全功能，使生产过程和制造过程可靠和安全。由于国内在功能安全技术的理论

和应用实践方面的研究都处于起步阶段，因此迫切需要加强这方面的工作，并迅速地在各行业中推广，以便跟上国际形势和贯彻执行国际标准。

功能安全技术从广义的角度来说，它涉及到可靠性工程、电气安全工程、环境适应性（包括电磁兼容性、机械振动、气候条件等）和电气通信等技术，涉及面很广，在工程上有很重要的应用。

本书共分8章，第1章功能安全概述；第2章可靠性和环境适应性技术基础（包括可靠性和环境适应性的基本概念、可靠性技术和环境适应性试验技术）；第3章危险、风险评估技术和方法（包括危险、风险的基本概念和评估技术及方法）；第4章E/E/PE安全相关系统的设计和开发，这是本书的重点，从设计和开发的目的以及要求开始，包括安全功能要求的分配、硬件安全完整性的要求（包括硬件故障裕度、硬件结构约束、硬件失效概率的评估等）、软件的要求以及安全生命周期实现各阶段的要求；第5章SIS应用软件功能安全生命周期的实现阶段；第6章安全生命周期的管理（包括管理要求、安全要求规范的制定和功能安全的认定）；第7章特殊场合用的安全装置及其安全相关系统的功能安全要求和SIL的评估（包括爆炸气体环境用安全装置功能安全要求和SIL的评估，有毒、有害气体探测系统的功能安全要求和SIL的评估）；第8章功能安全的应用（包括防爆隔离式安全栅功能安全和SIL的评估、某化工厂合成分离净化CO和$H_2$中安全仪表系统（SIS）的功能安全和SIL的评估、SIEMENS“SIMATICS7分布式安全装置”在机床安全保护系统中的应用）。

本书以GB/T 20438.1～.7（IEC 61508-1～-7《电气/电子/可编程电子安全相关系统的功能安全》内容为主要框架，并结合电子、过程领域、机械和特殊环境行业的具体情况及相关的国外资料来进行叙述。

本书对主要功能安全指标即SIL的计算方法和涉及可靠性方

面的内容进行了叙述和说明，内容丰富、深入浅出，通俗易懂，并具体举例说明功能安全指标即安全完整性等级（SIL）的评估方法。

本书由上海工业自动化仪表研究所、上海仪器仪表自控系统检验测试所和国家工业自动化仪表产品质量监督检验中心策划并组织编写。李佳嘉、谢亚莲、张艾森参加了本书的编写工作，本书的出版还得到了西门子（中国）有限公司自动化与驱动集团的支持，在此一并表示诚挚的谢意。

作者虽然长期从事可靠性及功能安全的研究工作，但编写本书是一个新的尝试，难免会存在不少问题和缺点，希望广大读者给予支持、帮助和批评指正。

**编　者**

2008 年 3 月

## 电气自动化

| 序号 | 书　名 | 书　号 | 定价 | 出版时间 |
|---|---|---|---|---|
| 1 | 计算机控制系统理论与应用 | 978-7-111-22981-0 | 26 | 200801 |
| 3 | 计算机测控系统与数据采集卡应用 | 978－7-111-22132-6 | 47 | 200710 |
| 7 | 数字伺服控制系统与设计 | 978-7-111-21609-4 | 40 | 200707 |
| 9 | 控制装置与仪表 | 978-7-111-21083-2 | 32 | 200704 |
| 10 | 最新工业自动化测控应用手册 | 978-7-111-21113-6 | 59 | 200704 |
| 13 | 现场总线与工业以太网 | 7-111-20097-7 | 20 | 200701 |
| 14 | 伺服运动控制系统的结构及应用(1CD) | 7-111-19832-8 | 30 | 200610 |
| 15 | 过程计算机控制及先进控制策略的实现 | 7-111-19268-0 | 33 | 200701 |
| 17 | 数字化工厂技术与应用 | 7－111-18668-0 | 30 | 200604 |
| 23 | 工业控制网络与现场总线技术 | 978-7-111-18421-8 | 28 | 200708 |
| 25 | 集散系统及系统开放 | 7-111-15582-3 | 33 | 200508 |
| 26 | 集散控制系统及其应用 | 7-111-17939-0 | 23 | 200601 |
| 27 | 电力遥视系统原理与应用 | 7-111-15557-2 | 30 | 200501 |
| 30 | 电气自动控制 | 7-111-15242-5 | 26 | 200702 |
| 31 | 工业控制计算机系统及其应用 | 978-7-111-23055-7 | 30 | 200803 |

## 仪器仪表

| 序号 | 书　名 | 书　号 | 定价 | 出版时间 |
|---|---|---|---|---|
| 1 | 2006/2007 传感器与执行器大全 | 978-7-111-23211-7 | 99 | 200801 |
| 2 | 现代传感器应用技术 | 978-7-111-19672-3 | 28 | 200709 |
| 3 | 压力测量技术及仪表 | 7-111-16598-5 | 20 | 200607 |

以上图书由全国各地新华书店经销。也可由中国科技金书网（www. golden-book. com）订购，联系电话：010-68993821、88379639、88379641。

# 目　录

前言
第 1 章　功能安全概述 …… 1
1.1　功能安全的重要性和国内外研究概况 …… 1
1.1.1　功能安全的重要性 …… 1
1.1.2　国外研究概况 …… 2
1.1.3　国内研究概况 …… 4
1.2　术语（缩略语）和定义 …… 5
1.3　安全生命周期概念 …… 12
1.3.1　目的 …… 15
1.3.2　要求 …… 16
第 2 章　可靠性和环境适应性技术基础 …… 17
2.1　可靠性和环境适应性的基本概念 …… 17
2.1.1　可靠性的基本概念 …… 17
2.1.2　环境适应性的基本概念 …… 18
2.2　可靠性特征量和常见的失效分布 …… 19
2.2.1　可靠性特征量 …… 20
2.2.2　产品的寿命特征 …… 30
2.2.3　几种常见的失效分布 …… 33
2.3　可靠性技术 …… 40
2.3.1　可靠性试验及其数据统计处理 …… 40
2.3.2　可靠性预计和可靠性分析技术 …… 55
2.4　环境适应性技术 …… 78
2.4.1　概况 …… 78
2.4.2　工业自动化仪表工作条件 …… 80
2.4.3　工业自动化仪表环境试验技术要求 …… 85
第 3 章　危险和风险评估技术和方法 …… 96
3.1　危险和风险的基本概念 …… 96

3.1.1 危险和风险 …… 96
3.1.2 安全与风险 …… 96
3.1.3 风险降低的一般概念 …… 96
3.2 危险和风险评估的目的 …… 98
3.3 危险和风险评估的要求 …… 99
3.4 风险评估技术和方法 …… 102
3.4.1 安全完整性与风险降低 …… 102
3.4.2 允许风险和 ALARP 模型 …… 103
3.4.3 安全完整性等级的定量确定方法 …… 106
**第 4 章 E/E/PE 安全相关系统的设计和开发** …… 126
4.1 目的 …… 126
4.2 要求 …… 126
4.3 SIS 在检测故障时的系统行为要求 …… 135
4.4 制定 E/E/PE 安全相关系统的安全要求规范 …… 136
4.4.1 制定目的 …… 136
4.4.2 制定 SIS 的安全要求 …… 136
4.4.3 制定机械的安全相关控制功能（$SRCF_S$）的要求规范 …… 140
4.5 E/E/PE 安全相关系统中硬件功能安全的实现和功能安全评估步骤 …… 141
4.5.1 E/E/PE 安全相关系统中硬件功能安全评估步骤 …… 141
4.5.2 安全相关电气控制系统（SRECS）硬件功能安全的实现步骤 …… 142
4.6 SIS 的安全功能分配 …… 144
4.6.1 分配目的 …… 144
4.6.2 分配要求 …… 145
4.6.3 安全完整性等级 4 的附加要求 …… 147
4.6.4 作为一个保护层的基本过程控制系统（BPCS）的要求 … 148
4.6.5 防止共同原因失效的要求及量化共同原因失效效应的方法 …… 148
4.7 硬件安全完整性要求 …… 152
4.7.1 硬件故障裕度要求 …… 152
4.7.2 硬件安全完整性的结构约束 …… 152
4.7.3 硬件随机失效概率的计算 …… 160

4.8 选择部件和子系统的要求 …… 178
4.9 软件的要求 …… 181
4.9.1 目的 …… 181
4.9.2 软件安全生命周期的要求 …… 181
4.9.3 软件安全生命周期各阶段的实现 …… 182
4.10 SIS 的现场设备要求 …… 183
4.11 SIS 的接口要求 …… 183
4.11.1 操作员接口要求 …… 183
4.11.2 维护/工程接口要求 …… 184
4.11.3 通信接口要求 …… 185
4.12 SIS 的操作、维护和测试 …… 185
4.12.1 操作和维护的要求 …… 185
4.12.2 集成测试和功能检验测试 …… 187
4.13 SIS 的安全验证、确认和评估 …… 192
4.13.1 安全验证 …… 192
4.13.2 安全确认 …… 192
4.13.3 功能安全评估 …… 196
**第 5 章 SIS 应用软件安全生命周期的实现阶段** …… 198
5.1 应用软件安全生命周期的要求 …… 198
5.2 应用软件安全要求的规范 …… 200
5.3 应用软件安全确认的计划 …… 203
5.4 应用软件的设计和开发要求 …… 204
5.5 应用软件与 SIS 子系统的集成 …… 217
5.6 固定程序语言（FPL）和有限可变语言（LVL）软件修改规程 …… 218
5.7 应用软件的验证 …… 219
5.8 安全软件的评估 …… 221
**第 6 章 安全生命周期的管理** …… 227
6.1 目的 …… 227
6.2 要求 …… 227
6.3 功能安全认证模式、认证过程和认证方法 …… 235
**第 7 章 特殊场合用安全装置及其安全相关系统的功能安全要求和 SIL 的评估** …… 236

7.1 概述 …… 236
7.2 爆炸性气体环境用安全装置的功能安全要求和 SIL 的评估 …… 236
7.2.1 概况 …… 236
7.2.2 爆炸性气体环境用安全装置的阻燃要求 …… 237
7.2.3 爆炸性气体用安全装置的功能要求 …… 238
7.2.4 爆炸性气体用安全装置中安全部件的特殊要求 …… 239
7.2.5 爆炸性气体用安全装置的功能安全要求 …… 240
7.2.6 爆炸性气体用安全装置的型式试验和例行试验 …… 242
7.2.7 爆炸性气体环境用安全装置安全完整性等级（SIL）的评估 …… 243
7.3 有毒有害气体探测系统的功能安全要求和 SIL 的评估 …… 244
7.3.1 概况 …… 244
7.3.2 固定式气测系统的安全功能要求 …… 244
7.3.3 模块与元件的特性和要求 …… 248
7.3.4 安全功能特性 …… 263
7.3.5 固定式气体探测系统 SILC 的确定程序 …… 269
**第 8 章 功能安全的应用** …… 278
8.1 功能安全评估的应用实例 …… 278
8.1.1 防爆隔离式安全栅功能 SIL 的评估 …… 278
8.1.2 某化工厂合成分离净化 CO 和 $H_2$ 装置中的 SIS 功能安全和 SIL 的评估 …… 280
8.2 SIEMENS SIMATIC S7 分布式安全装置在机床安全保护系统中的应用 …… 286
8.2.1 机床及其安全相关控制系统的特征和安全相关控制功能 …… 286
8.2.2 风险分析和判定 SRCF 要求的 SIL …… 287
8.2.3 制定机床 SRECS 的 SRCF 规范 …… 289
8.2.4 SRECS 的结构设计 …… 289
8.2.5 SRECS 子系统的实现 …… 291
8.2.6 结论 …… 299
**附录** …… 300
附录 A 现场工作报告 …… 300
附录 B 计划维修级别分类 …… 301

附录 C　失效分析报告 …… 301
附录 D　定数截尾 MTBF 双侧（或单侧）置信限系数 $C_L$、$C_U$ …… 302
附录 E　定时截尾 MTBF 双侧（或单侧）置信限系数 $C_L$、$C_U$ …… 303
附录 F　$\chi^2$ 分布分位数表 …… 304
附录 G　中位序表 …… 306
附录 H　可靠性预计分析汇总表 …… 307
附录 I　可编程电子或传感器或最终元件的评分 …… 307
附录 J　$Z$ 的值：可编程电子 …… 311
附录 K　$Z$ 的值：传感器或最终元件 …… 312
附录 L　$\beta$ 和 $\beta_D$ 的计算 …… 312
附录 M　检验测试时间间隔为 6 个月，平均恢复时间为 8h 时要求的平均失效概率 …… 313
附录 N　检验测试时间间隔为 1 年，平均恢复时间为 8h 时要求的平均失效概率 …… 316
附录 O　检验测试时间间隔为 2 年，平均恢复时间为 8h 时要求的平均失效概率 …… 319
附录 P　检验测试时间间隔为 10 年，平均恢复时间为 8h 时要求的平均失效概率 …… 322
附录 Q　检验测试时间间隔为 1 个月、平均恢复时间为 8h 时每小时的平均失效概率（高要求或连续操作模式下） …… 325
附录 R　检测测试时间间隔为 3 个月，平均恢复时间为 8h 时每小时的平均失效概率（高要求或连续操作模式下） …… 328
附录 S　检验测试时间间隔为 6 个月，平均恢复时间为 8h 时每小时的平均失效概率（高要求或连续操作模式下） …… 331
附录 T　检验测试时间间隔为 1 年，平均恢复时间为 8h 时每小时的平均失效概率（高要求或连续操作模式下） …… 334
附录 U　电源指示设备中电子元器件失效模式及其比率的例子 …… 337
**参考文献** …… 341

# 第1章　功能安全概述

## 1.1　功能安全的重要性和国内外研究概况

### 1.1.1　功能安全的重要性

工业过程成套设备以及其他设备在工作不正常的情况下有可能产生诸如火灾、爆炸、辐射超剂量、机械漏油等危险事件，因此对人和环境存在一定的风险。

在国外，由于各种重大事故引发出问题的焦点是功能安全，例如，前苏联的切尔诺贝利核电站事故；1984 年博帕尔农药厂甲基异氰酸盐泄漏，导致 6400 人死亡，13.5 万人受到伤害，20 多万人被迫迁移。

我国目前正处于经济和社会的转型期，面临经济与社会发展严重失衡的局面，各种安全事故的不断发生，如由于煤矿无序地开发和管理以及片面地追求经济效益，致使煤矿的渗水、煤层坍方等事件相继发生，我国百万吨煤死亡率是美国的 160 倍、印度的 10 倍。从 1990 年到 2005 年我国因生产安全事故导致死亡的人数令世界震惊（见图 1-1），由于事故的不断发生，致使企业生产停顿，甚至破产，造成社会秩序混乱，这已成为我们构建和谐社会进程中不和谐音。

同样，在我国各种工业控制应用领域的运行过程中，存在着许多潜在的危险和风险，包含的复杂性也各不相同，其中很多功能安全是通过采取被动的系统措施获得的，较少部分功能安全是通过安全系统主动获得的，这就需要提高应用不同的安全保护系统，获得更多的主动的系统保护功能。但是，安全保护系统本身在功能安全方面必须达到规定的安全要求，具有合理的安全完整性水平，才能保证安全保护系统、受控设备和受控设备控制系统

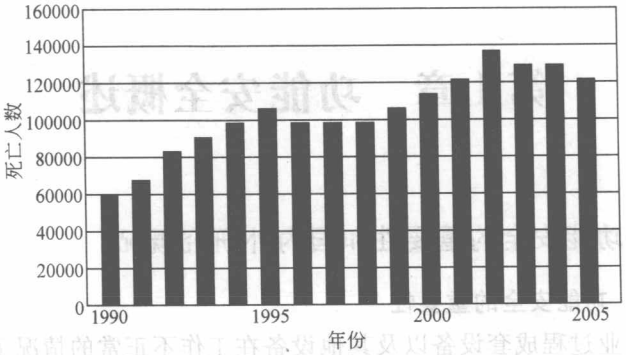


图 1-1　1990～2005 年我国因生产安全事故导致死亡人数的统计

安全正常地工作。

### 1.1.2　国外研究概况

由现场传感器或/和变送器（如温度变送器、压力变送器、位置开关等）、控制器（如可编程序/控制器、现场总线等）、输入/输出模块和现场执行机构（如电磁阀、电动调节阀、接触器等）组成，并与相应的输入输出接口（如隔离式安全栅）及相关软件一起构成安全仪表系统（Electrical/electronic/Programmabale electronic，Safety Instrumented System，SIS）或安全相关电气控制系统（Safety—Related Electrical Control System，SRECS）。在电力、机械、化工、航天航空、核能、医药等领域有着广泛的应用，应用范围也在不断地扩大。由于应用场合大多数是系统结构复杂、容易爆炸、操作自动化程度较高、生产产品质量要求很高的场合，同时，用户对使用要求的不断提高，尤其是在受控设备功能安全性上提出了更高的要求。因此，根据用户的这种要求和实际需要以及科学技术的发展，近几年来，SIS 和 SRECS 也得到了飞速发展。从第一代模拟式系统，经过第二代智能系统，发展到现在的第三代数字智能式系统。

国外首先对电气/电子/可编程电子相关系统（Electrical/electronic/Programmabale electronic，Safety Instrumented System，E/E/PES）功能安全的基础标准开展了研究，并在该标准的基

础上，又对其他应用部门的安全相关系统的功能安全进行了研究，建立了功能安全的标准体系（见图 1-2）。特别是美国和欧共体国家在这方面进行了大量的研究，制定了许多功能安全领域的标准（如 DIN V 19250/VDE V 0801、ANSI/ISA S84.01（USA）、EN61508 等），1998 年国际电工委员会（IEC）颁发了国际标准 IEC 61508-1-7《电气/电子/可编程电子安全相关系统的功能安全》，2003 年和 2005 年国际电工委员会（IEC）针对过程工业领域测控仪表及其系统和机械装置又颁发了国际标准 IEC 61511-1-3《过程工业领域安全仪表系统功能安全》和 IEC 62061《机械安全-电气/电子/可编程电子安全相关控制系统的功能安全》。这些标准的建立，为过程工业领域 SIS 和机械-安全相关控制系统（SRESC）在各种应用场合的可靠、安全使用打下良好基础。

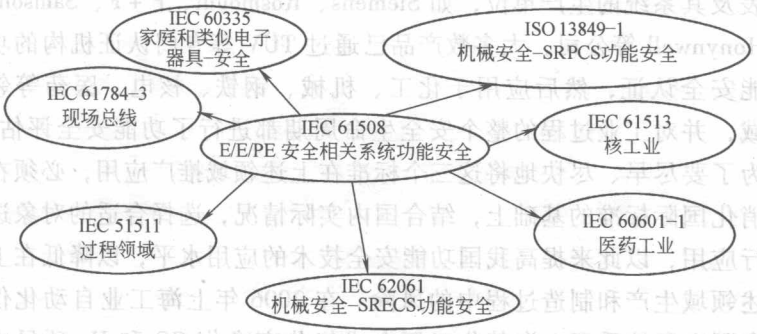


图 1-2　功能安全的标准体系

目前，欧共体的主要发达国家不但对自身产品提出了功能安全的要求，而且，对进入欧共体国家的产品也已提出了功能安全的要求，几乎主要制造仪表及系统的公司（如 Siemens、Honeywell、Rosemont、P + F、Samson 等）都有定量的安全完整性（SIL）指标的要求，可以自身进行功能安全评估，对于 SIL 指标要求高的产品，都要交给第三方专门的评估机构（如 TÜV、Sira 等）进行功能安全认证，这样，既保证了产品的功能安全，又减少产品在使用过程中发生事故的可能性。

### 1.1.3 国内研究概况

在国内，2004 年由仪器仪表综合技术研究所在十五标准化项目中，开始对 IEC 61508-1-7 和 IEC 61511-1-3 标准进行等同翻译，2006 年制定了国家标准 GB/T 20438.1-7—2006《电气/电子/可编程电子安全相关系统的功能安全》；2007 年制定了 GB/T 21109.1-3—2007《过程工业领域安全仪表系统功能安全》。遗憾的是，国内对上述标准进行相应的应用研究工作刚刚起步，还需要深化研究并扩大应用范围。

上海工业自动化仪表研究所自 2005 年开始，对 IEC 61508、IEC 61511 和 IEC 62061 标准进行了研究，其主要目的是把这三个国际标准应用于国内。通过对网上查找的情况看，国外非常重视功能安全的应用工作，而且已经很普及，尤其是测量与控制仪表及其系统的生产单位，如 Siemens、Rosmount、P + F、Samson、Honynwell 等公司，大多数产品已通过 TÜV 等专门认证机构的功能安全认证，然后应用于化工、机械、钢铁、核电、医药等领域，并对工业过程的整个安全生命周期都进行了功能安全评估。为了要尽早、尽快地将这三个标准在上述领域推广应用，必须在消化国际标准的基础上，结合国内实际情况，选择合适的对象进行应用，以此来提高我国功能安全技术的应用水平，以降低在上述领域生产和制造过程中的风险。在 2006 年上海工业自动化仪表研究所接受了上海某化工厂合成气分离净化 CO 和 $H_2$ 项目中八条安全保护控制系统功能安全要求中对 SIL 的项目评估，该项目是引进德国 Linde 公司的设备，德国 Linde 公司首先对生产过程中的危险和风险进行了评估，并要求上海工业自动化仪表研究所对所有安全保护系统进行了功能安全评估。所以，从 2006 年开始，该所首先对该项目的系统进行熟悉，并从各方面了解系统中所有仪表和系统的配置，并进行失效模式、影响和后果分析（FMEDA），对要求的失效概率（PFD）和安全失效分数（SFF）进行计算，最后根据德国 Linde 公司提出的每条安全保护系统功能安全中 SIL 的目标要求进行比较，得出评估结论。

由于国外对设备和系统功能安全的严格要求（在引进产品和系统中不断地体现），并且随着国际和国家相关标准的发布，各设计研究院已经开始重视设备和相关系统的功能安全要求，相信我国的设备和系统功能安全评估工作一定会得到迅速的发展。

## 1.2 术语（缩略语）和定义

1. 电气/电子/可编程电子（E/E/PE）和电气/电子/可编程电子系统（E/E/PES）

E/E/PE 是指基于电气（E）和/或电子（E）和/或可编程电子（PE）的技术。

E/E/PES 是指一个或多个 E/E/PES 装置的用于控制、防护或监视的系统，包括系统中所有的元素，如电源、传感器和其他输入装置，数据高速公路和其他通信途径，以及执行器和其他输出装置，如图 1-3 所示。

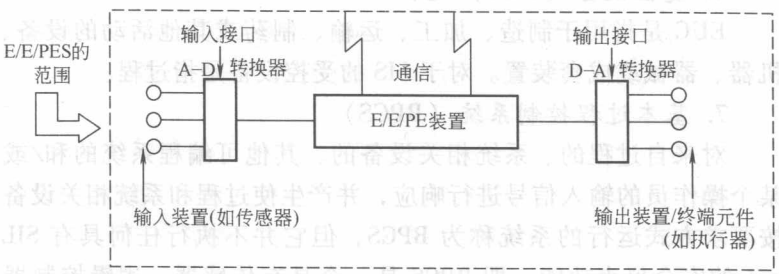


图 1-3 E/E/PES 的结构和术语

2. 安全仪表系统（SIS）

SIS 是指用来实现一个或几个安全仪表功能的仪表系统，SIS 可以由传感器、逻辑控制器和最终器件的任何组合组成。它可包含安全仪表控制功能，也可包含仪表安全保护功能，可以包括或不包括软件。

3. 安全相关电气控制系统（SRECS）

SRECS 是指所有机械控制系统的电气、电子和可编程电气部分，主要用来提供操作控制、监视、内锁、通信等的保护和安