安全仪表系统的功能安全

阳宪惠 郭海涛 编著

清华大学出版社

阳宪惠 郭海涛 编著

安全仪表系统的功能安全

清华大学出版社
北京

内 容 简 介

本书以石油化工等流程工业中广泛采用的安全仪表系统为对象，介绍安全仪表系统功能安全的相关理论、方法与技术。全书以安全生命周期为主线，围绕在设计、实施、评估、运行、维护环节如何提高安全仪表系统的安全性、可用性展开讨论。书中介绍了功能安全的概念和基本术语；安全仪表系统的组成、冗余结构、典型解决方案；失效模式、失效数据。阐述了系统风险分析、可靠性建模、安全完整性水平选择的相关方法。提供了典型石化单元安全仪表功能的设计、分析、性能指标计算，以及改进设计的相关示例。

本书力图内容深入浅出，图文并茂，在讲述功能安全基本原理方法的同时，也注重与工程实际应用相结合。

本书可作为高等院校自动化类专业、与安全仪表系统相关的理工科其他专业的教学参考书，也可作为安全仪表系统设计人员、流程工业安全技术人员的培训教材或参考书。

图书在版编目(CIP)数据

安全仪表系统的功能安全/阳宪惠，郭海涛编著. —北京：清华大学出版社，2007.10
ISBN 978-7-302-15298-9

Ⅰ. 安…　Ⅱ. ①阳…②郭…　Ⅲ. 仪表－安全　Ⅳ. TH7

中国版本图书馆 CIP 数据核字(2007)第 073833 号

责任编辑：王一玲
责任校对：梁　毅
责任印制：杨　艳
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 刷 者：清华大学印刷厂
装 订 者：三河市兴旺装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：15.5　**字　数**：364 千字
版　　次：2007 年 10 月第 1 版　　**印　　次**：2007 年 10 月第1 次印刷
印　　数：1～3000
定　　价：29.00 元

序

安全需求是人类生存和发展的基本需求之一。安全生产是经济社会发展的基础、前提和保障，必须纳入我国现代化建设的总体战略，与经济建设和社会发展各方面的工作同时规划、统一部署、同步推进。在我国工业化快速发展过程中，生产事故的风险问题或称安全生产问题已成为全社会普遍关注的重要问题之一，迫切需要通过安全科技和管理创新，促进安全管理水平的提高和社会经济的可持续发展。

现代工业生产的大规模发展，在为人类提供更丰富的物质生活产品的同时，也带来了灾难性事故危害。20 世纪 70 年代以来，由于生产过程安全系统失效，引发了一系列火灾、爆炸、毒物泄漏等事故灾难，造成了巨大的生命、财产损失和环境破坏。因此，如何预防重大工业事故成为各国社会、经济和科技发展的重点研究对象之一，受到了国际社会的广泛重视。功能安全是以保障安全系统能正确有效地执行其安全功能为目的，基于对安全系统整个生命周期风险分析和功能要求分配的安全技术，是安全科学与工程和控制科学与工程的交叉学科，是近 10 年来安全管理学和安全监控技术的新发展。国际电工组织(IEC)于 1998～2004 年先后发布了针对电气/电子/可编程电子安全相关系统的功能安全基础标准 IEC 61508 和针对过程工业的功能安全标准 IEC 61511。功能安全系列国际标准的发布表明，作为一个新的学科，功能安全已经开始形成体系并进入实际应用阶段。

近年来，我国已等同采用上述国际标准，但在功能安全相关理论和技术方面的研究、应用仍处于起步阶段。阳宪惠教授及其合作者在系统研究国内外功能安全技术进展的基础上，结合多年从事过程工业控制的相关研究成果，编著了《安全仪表系统的功能安全》。本书系统地论述了安全仪表系统功能安全的相关理论、技术和方法，提供了多类安全仪表系统功能安全分析、设计和评估的应用实例，为安全仪表系统设计、开发和基于功能安全思想的安全管理工作提供了基本的理论依据和技术方法。本书的出版必将为推动我国功能安全技术的研究和应用，提高我国工业安全管理和安全控制技术水平起到积极的促进作用。

吴宗之

中国安全生产科学研究院

2007 年 4 月

前　言

包括安全仪表系统在内的安全系统，是保障生产安全的重要措施，其自身的功能安全问题已经受到人们的广泛关注。功能安全是近年来发展形成的一套全新安全技术理念与管理方法，是对传统安全管理方式的一种突破。采用功能安全技术的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。

功能安全技术以系统在安全生命周期各阶段的安全完整性水平为核心，通过对受控过程进行危险与风险分析，为其设置有效的安全功能，选择恰当的目标安全完整性水平，设计出满足目标安全完整性水平要求的安全功能。通过安全仪表系统的作用，把受控过程的风险降低到一个可以接受的水平。功能安全技术为安全系统的设计、安装、评估、维护、直到停用的整个过程，提供了一整套行之有效的科学方法。

自 2000 年 IEC 61508 功能安全标准问世以来，作者一直在关注国内外该领域的技术发展动向并从事相关研究，《安全仪表系统的功能安全》一书正是作者对近年来研究工作和技术资料进行总结的基础上形成的。全书共分 12 章，围绕提高安全仪表系统的安全性、可用性问题展开讨论。从介绍安全仪表系统的功能安全、安全完整性水平、可靠性、可用性等基本概念和术语入手，讨论了安全仪表系统的组成、冗余结构、可靠性指标、失效模式、失效数据等；阐明了在系统风险分析、可靠性建模、安全完整性水平选择中所应用的相关基础知识与计算方法；分析了功能安全的相关因素；提供了典型石化单元安全仪表功能的典型解决方案，以及如何进行改进设计的相关示例。书中主要章节的初稿由郭海涛执笔，第 11 章的初稿由工程师徐玉娟执笔，张斌等也为本书的编写做了大量工作。

本书在其内容取材及编写过程中，作者力图理论联系实际，在讲述功能安全基本原理方法的同时，注重与工程应用相结合，使编写内容尽可能适合工程应用的实际需要。希望本书能为推动我国功能安全技术的发展，为提高我国工业生产安全水平起到积极作用。

安全仪表系统功能安全的研究在我国还刚刚开始。功能安全技术本身也还在发展过程之中。由于编著者水平有限，对该项技术的理解还不够深入，加上时间仓促，书中的缺点在所难免，恳请读者批评指正。

作者开展的安全仪表系统的功能安全的研究工作，以及本书的出版，得到了国家自然科学基金项目（项目编号：60674064）和国家科技支撑计划（2006BAK01B02-04-2）的支持，在此一并表示诚挚的谢意。

阳宪惠

2007 年 2 月于北京 清华园

目　录

第 1 章　安全仪表系统概述

1.1 引言

安全对经济、环境和人类自身的健康发展至关重要，因而安全相关系统（Safety-Related Systems）被广泛应用于生产过程之中。安全相关系统监视生产过程的状态，在危险条件出现时采取相应措施，防止危险事件发生，避免潜在危险对人身、设备、环境造成伤害或减轻其后果造成的损失。安全阀、安全气囊、火灾消防喷淋装置等，都是常见的安全相关系统实例。本书重点讨论的安全仪表系统（safety instrumented system，SIS）是安全相关系统的一个专门类别。它是在石油化工等流程工业中被广泛采用的、由仪表构成的一类安全相关系统，也被称为仪表型安全系统，或面向安全的仪表系统。

印度博帕尔毒气泄漏、前苏联切尔诺贝利核电站爆炸等震惊世界的灾难使人们前所未有地重视工业生产中的安全问题。安全相关系统是保障生产安全的重要措施，应能在危险发生时正确地执行其安全功能。但由于系统结构、硬件、软件及周围环境等原因，安全系统本身会不可避免地存在着安全性问题。在 2000 年由国际电工委员会（IEC）发布的 IEC 61508 标准（电气/电子/可编程电子安全系统（E/E/PES）的功能安全）中，明确提出了安全相关系统的功能安全（functional safety）问题，即当生产过程在出现危险条件时，安全相关系统能否有效执行其安全功能，如何提高其执行安全功能能力等相关问题。

安全相关仪表系统的安全功能（safety related function）指对某个具体的潜在危险事件实行的保护措施。如某管道或容器在出现超高压情况时的泄流或停车；某加热炉出现超高温情况时灭火等，都分别属于一个安全功能。而功能安全则指安全功能本身的安全性，用于描述安全相关系统执行其安全功能的能力。本书以安全仪表系统为主要对象，讨论保障其功能安全的相关理论、方法与技术。安全仪表系统的功能安全问题，属于安全工程的学科范围。

早在 20 世纪 40 年代中期，美国军方就开始研究可靠性和安全工程。近年来在北美、欧洲、日本等地，围绕安全相关系统功能安全管理这一新的课题，从相关理论方法研究、标准规范建立，到实际安全系统的设计、分析、实施、评估、认证，已经开展了一系列的研究工作，取得了大量有价值的成果。一些有关功能安全分析评估的著作也相继出版。自 IEC 61508 发布后，不同应用领域的功能安全标准陆续出台：IEC 61511、IEC 61784—3、IEC 62061、IEC 60204—1等，IEC 功能安全标准系列正在形成。在功能安全标准的推动下，与功能安全相关的技术与产品开发也十分活跃。

早期的执行安全功能的安全相关系统大多是由继电器搭建的安全联锁系统。它能够

很出色地完成对系统的保护功能，而且可靠性相当高。但是继电器安全联锁系统的最大缺陷就是维护相当烦琐，对其安全功能进行改动非常困难。因此，包括安全仪表系统在内的现代安全相关系统，大都采用基于可编程电子器件的构成方式。这样的系统除了具有很高的可靠性之外，还具有易于维护和改动，适用于大规模应用等优势。

基本过程控制系统(basic process control system)和安全仪表系统是在流程工业中广泛采用的两种不同类型的系统。基本过程控制系统执行基本过程控制功能，使生产过程的温度、压力、流量、液位等工艺参数维持在规定的正常范围之内，以保证产品的产量与质量；安全仪表系统则监视控制系统的状态，判断危险条件，防止危险发生或者减轻事故造成的后果。安全仪表系统和基本过程控制系统的被控对象都是生产过程。

一个安全仪表系统可以执行多个安全仪表功能(safety instrumented function，SIF)。每一个安全仪表功能针对特定的风险对生产过程进行保护。安全仪表系统必须在生产过程出现危险情况时正确执行其对应的安全仪表功能，这一点对于工业过程的安全是非常重要的。本书中安全仪表功能与安全功能两个概念对于安全仪表系统是等同的。

在一定时间、一定条件下，安全仪表系统能成功地执行其安全功能的概率，被称为安全完整性水平(safety integrity level，SIL)，其数值代表着安全仪表系统使过程风险降低的数量级。安全仪表系统的功能安全技术，通过对受控过程进行危险与风险分析，确定正确的安全功能，选择恰当的目标安全完整性水平，设计满足目标安全完整性水平的安全仪表功能。通过对安全仪表系统的功能安全水平实行测试、评估、认证等，把受控过程的风险降低到一个可以接受的水平。功能安全管理为安全系统从设计、安装、验证评估到维护、停用的整个安全生命周期的安全提供了一整套行之有效的科学方法。本书将围绕上述内容展开讨论。

1.2 安全仪表系统及其构成

什么是安全仪表系统呢？按照 IEC 61511 中的定义，安全仪表系统是由传感器、逻辑控制器和执行器组成的、能够行使一项或多项安全仪表功能的仪表系统。考虑一个压力容器的简单例子。为了防止该容器内压力超过额定值而发生爆炸，所以安装了一个安全仪表系统。该安全仪表系统由一个压力变送器、一个阀门和一个 PLC 组成，如图 1.1 所示。图 1.1 中的安全仪表系统的工作也十分简单。压力变送器检测容器内压力并将其变换成合适的信号传送给 PLC，PLC 判断若压力超过了额定值则打开阀门以降低容器内压力。这被称为安全仪表系统的一个安全仪表功能。很明显本例子中安全仪表系统只有一个安全仪表功能。对于这个例子，组成系统的 3 个设备中只要有一个发生故障而失效，那么安全仪表系统的安全仪表功能将失效。换句话说，安全仪表系统将不能对压力容器内的压力进行限制，也就是不能达到保障安全的目的。

设计一个安全仪表系统时，应该使该安全仪表系统具有正确的安全功能。此外，必须考虑安全仪表功能能够多好地被执行。在上面的例子中，压力变送器每个月一次的故障率和每年一次的故障率将使安全仪表系统的安全性能差异很大。安全完整性水平关心的就是安全功能能够多好地得到执行。

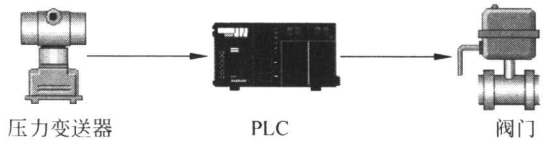

图 1.1　安全仪表系统示例

安全仪表系统的功能包括：

(1) 监视生产过程的状态，判断生产过程是否出现发生某种潜在危险的条件。

(2) 当出现危险的条件时，自动执行其规定的安全仪表功能，防止危险事件发生。换句话说，安全仪表系统一旦执行了其安全仪表功能，则将没有危险事件发生。

(3) 减轻危险事件造成的影响，即通过减少损失或减轻影响后果的办法来降低风险。

在一些情况下，安全仪表系统实现安全仪表功能的目的是减小风险，或者说是减小潜在危险发生的概率；在另外一些情况下，实现其安全仪表功能的目的是减弱已发生的危险事件的后果；还有一些情况下，则是两种情况的综合。

1.3　安全仪表系统与基本过程控制系统

基本过程控制系统是执行常规正常生产功能(如 PID 控制、积分控制等)的控制系统。这里的基本过程控制系统与执行过程优化等复杂“高级”过程控制的系统相对应。据统计，工业中 95%以上的控制系统都是基本过程控制系统。由此可看出，基本过程控制系统执行基本生产控制功能，以达到生产过程的正常操作要求。

安全仪表系统则监视生产过程的状态，判断危险条件，防止风险的发生或者减轻风险造成的后果。因此，一个生产过程应该具备过程控制系统和安全仪表系统这两类不同功能的系统。基本过程控制系统用来执行系统的基本控制功能，而安全仪表系统则监视生产过程的状态，以保证整个系统的安全运行。图 1.2 表示了为某反应器设置的过程控制系统和安全仪表系统。

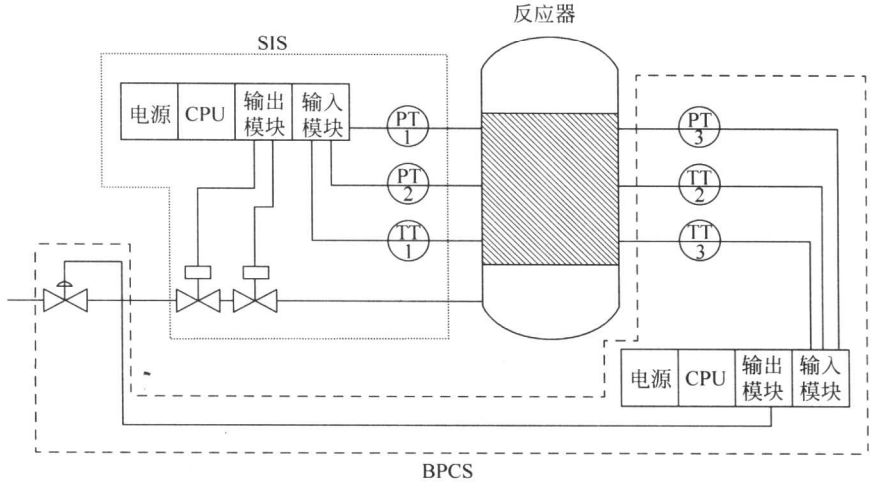

图 1.2　SIS 和 BPCS

显而易见，基本过程控制系统与安全仪表系统的功能完全不同。基本过程控制系统执行基本过程控制功能以达到生产过程的操作要求；安全仪表系统则监视生产过程的状态，判断是否出现危险条件，防止风险的发生或者减轻风险发生后造成的后果。基本过程控制系统是主动的、动态的。因为基本过程控制系统是用来满足生产需要的，因此，它必须根据系统的设定要求和生产过程的扰动状态不断地动态运行，才能保持生产过程的连续稳定运行。一旦其运行终止，则整个生产过程也就随之失去控制。

相反，安全仪表控制系统则是被动的、休眠的。在基本过程控制系统正常运行时，安全仪表系统一般是处于静态的。它在很长一段时间里都会处于“休眠”状态，而且理想状态是它能一直“休眠”下去。因为，安全仪表系统处于“休眠”状态，正表明了基本过程控制系统控制下的生产过程的安全运行。例如，对于一个减压阀，在正常情况下，它是处于关闭状态的。只有在出现危险条件，即当压力超过一定的极限标准时，安全仪表系统才会动作，即减压阀才会打开。如果压力永远都不会超过极限标准，那么减压阀永远都不会发挥作用，而是一直处于“关闭”的“休眠”状态。但是如果压力超标时，减压阀因为失效而不能打开，那么安全仪表系统就发生了要求时失效。要求时失效的概率和安全完整性水平是紧密联系的。

对于基本过程控制系统来说，其大部分失效都是显而易见的。例如，在自动化生产线上的机器人，其职责是把放在地点 A 的物体挪到地点 B。如果他把地点 B 的物体挪到了地点 A，就发生了一个显而易见的系统失效。再如，某工业过程中的控制阀发生了故障，即不能在需要的时候达到特定的开关状态，那么，必定会影响正常的生产过程，由此产生的故障现象会立刻显现出来。即对于基本过程控制系统来说，其失效会在生产的动态过程中自行显现，很少存在“隐藏”的失效。

安全仪表系统的失效就没有那么明显了。这是由安全仪表系统的运行方式所决定的。正是由于安全仪表系统大部分时间是处于“休眠”状态，所以很难觉察它是否出现了失效或存在的问题。就好比是一个人无法知道扔在地下室里的备用发电机在需要的时候是否还能正常运行；无法知道 7 年没工作过的限压阀在某天突然超压时是否还能起到限压的作用。正因如此，确定休眠系统是否还能正常工作的唯一方法，就是对该系统进行周期性的诊断或测试。因此，安全仪表系统需要人为地进行周期性的离线或在线测试，而有些安全系统则带有内部的自诊断测试系统。

1.4 功能安全

功能安全(functional safety)是安全仪表系统是否能有效地执行其安全功能的体现。一个安全仪表系统可以具有多个安全仪表功能，每一个安全仪表功能针对特定的风险对工业过程进行保护。安全仪表系统必须在工业系统出现危险情况时正确执行其对应的安全仪表功能，这一点对于确保工业过程处于安全状态是非常重要的。安全仪表系统的这种特性被称为功能安全。安全仪表系统的功能安全水平高，意味着该安全仪表系统能正确有效地执行其安全功能的能力强，即能较大程度地减小风险发生的概率。

功能安全基础标准 IEC 61508 在起草阶段就已经受到了人们的广泛关注。通过对其

中的一些概念和方法的分析，解决了困扰多年的对以电气、电子、可编程电子技术为基础的安全相关系统安全保障的理论与实践问题。IEC 61508 提出了一种保证安全的哲学思想方法和科学的安全管理程序，同时能更有效地节约成本。很多国家已经将功能安全标准定为强制性标准。

1.5　安全生命周期

在 IEC 61508 和 IEC 61511 中都提出了安全生命周期(safety life cycle，SLC)的概念。安全生命周期的定义为：在安全仪表功能(SIF)实施中，从项目的概念设计阶段到所有安全仪表功能停止使用之间的整个时间段。在安全生命周期内要进行一系列必需的活动。安全仪表系统整体的安全生命周期从其概念开始，经历若干中间阶段一直到安全系统停用，包括了为达到必需的安全完整性水平而进行的一切活动。换句话说，安全生命周期包括了安全仪表系统在概念、设计、运行、测试、维修及停用各阶段的所有活动，以达到高水平的功能安全。达到功能安全不是一劳永逸的，而是一个持之以恒、无微不至的过程。例如，安全仪表功能不但应该正确，还必须要有适当资格的人员对其进行正确的周期性测试，才能保证安全性以及正常生产的顺利进行。再例如，错误的安装可能不会在开车时被发现，但却给运行安全埋下了隐患。因此，采用安全生命周期的方式进行功能安全管理的关键思想是，从最初始的概念设计阶段一直到最后的停用活动，都自始至终地贯穿“安全”的概念。若其中任何一个环节的活动出现问题，都可能造成“千里之堤，溃于蚁穴”的后果。

那么，为什么需要安全生命周期呢？目的很显然，是为了达到较高的功能安全水平，更大程度地减小风险。这就好比做菜需要有个菜谱，做实验需要有份实验指导书，安全生命周期用系统的方式建立一个框架，用以指导安全仪表系统的设计和评价。依据安全生命周期的各项活动要求实施的安全仪表系统，才能最大程度地减小工业过程中的风险，降低安全仪表系统中存在系统性不足的概率。安全仪表系统的硬件随机失效则可以通过安全完整性水平来衡量。

安全完整性水平贯穿于安全系统生命周期的始终。安全系统的安全完整性水平不仅是安全系统安全性能的度量标准，而且是安全系统生命周期中的主线，将安全系统整体生命周期的各个阶段联系起来。安全完整性水平使得整体安全生命周期这个大框架下的所有活动能够具有良好的一致性。另一方面，如果不采用安全生命周期的方式来进行功能安全管理，那么是很难保证安全完整性水平能够达到目标要求的。

1.5.1　安全生命周期的各项活动

安全生命周期分为 3 个阶段：分析阶段、实现阶段和运行阶段。图 1.3 为 IEC 61508 标准中对整体安全生命周期的描述。该图提供了安全生命周期中各阶段的详细活动。从图中可以看出，各阶段的活动之间并不是孤立存在的，它们实际上是一个完整的体系，相互之间有一定的逻辑关系和顺序。例如，只有在“危险和风险分析”完成之后，才能确定