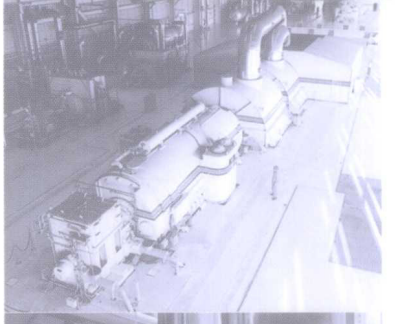
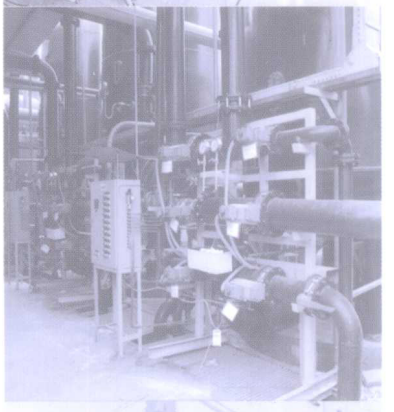
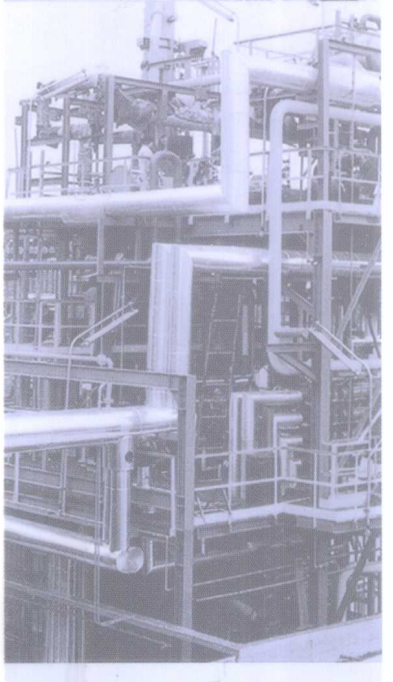
The Application of
Safety Instrumented Systems
for the Process Industry Sector

安全仪表系统
在过程工业中的应用

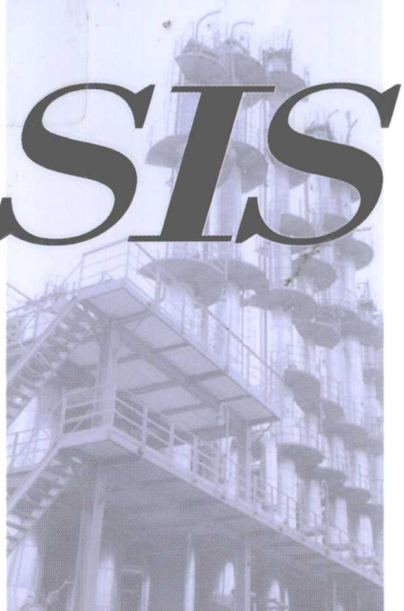
张建国　编著







SIS



中国电力出版社
www.cepp.com.cn

The Application of Safety Instrumented Systems for the Process Industry Sector

安全仪表系统在过程工业中的应用

张建国　编著

中国电力出版社
www.cepp.com.cn

内 容 提 要

本书循着 IEC61508/IEC61511 安全生命周期的脉络，以 SIS 在过程工业的应用为主题，全面解读这些功能安全标准的内涵和要求，指导 SIS 的工程实践。全书共分 11 章。第 1 章对全书中涉及到的一些关键概念做概括性介绍；第 2 章介绍在过程工业的 SIS 应用中有代表性的功能安全标准；第 3～6 章，围绕着 SIS 的安全生命周期各阶段的活动，介绍危险和风险分析、安全保护层以及 SIF 的 SIL 确定、SIS 的工程设计；第 7 章介绍 SIS 的核心子系统—逻辑控制器（Logic Solver）；第 8 章介绍 SIS 的现场安装、调试及维护；第 9 章介绍 SIS 的典型应用；第 10 章就 IEC61508/IEC61511 应用中的典型问题作比较深入的专题探讨；第 11 章介绍 IEC62061 和 IEC61513 的要点。

本书适合过程工业领域自控设计、应用、维护人员及安全管理人员阅读，也可作为高等院校自动化及相关专业，与安全仪表系统相关的理工科其他专业的教学参考书。

图书在版编目（CIP）数据

安全仪表系统在过程工业中的应用/张建国编著．—北京：中国电力出版社，2010.6

ISBN 978-7-5123-0234-1

Ⅰ.①安… Ⅱ.①张… Ⅲ.①仪表—应用—安全技术 Ⅳ.①X93

中国版本图书馆 CIP 数据核字（2010）第 047850 号

中国电力出版社出版、发行

（北京三里河路 6 号 100044 http://www.cepp.com.cn）

北京市同江印刷厂印刷

各地新华书店经售

*

2010 年 7 月第一版 2010 年 7 月北京第一次印刷

787 毫米×1092 毫米 16 开本 18.25 印张 444 千字

定价 **39.00** 元

序

我第一次接触功能安全这个概念是在 1999 年，当时我刚刚接手全国工业过程测量和控制标准化技术委员会 TC124 主任委员的工作，带队到南非参加国际电工委员会/工业过程测量和控制标准化技术委员会（IEC/TC65）的年会。会上，IEC61508《电气/电子/可编程电子安全相关系统的功能安全》标准起草工作组的组长荣倍先生找到我，告知我功能安全这个标准非常重要，希望中国也能够参与其中的工作。我从此进入了功能安全工作，并带领一个团队用了三年的时间将 IEC61508 转化成为了中国国家标准。标准一经发布即产生了极大的反响，社会各方都极为重视。由于功能安全是个既新且牵扯面又很广的概念，难以让人们在短时间内迅速了解，所以 TC124 办了十几期的培训班。在上课的过程中，我一直感到仅就概念进行介绍是远远不够的，我们缺少一位即有扎实的理论根基又有丰富实践经验的人，直到我遇见了本书的作者张建国先生。

张建国先生从事安全工作多年，具有长期的一线实践且具备丰厚的理论基础，是TÜV认证的功能安全专家。之后我们开始了很好的合作。至今张建国先生已为我国培养了几批经TÜV认证的安全工程师。

本书循着 IEC61508/IEC61511 安全生命周期的脉络，围绕 SIS 在过程工业中的应用，解读这些功能安全标准的内涵和要求，指导如何进行 SIS 工程实践。本书具有如下特点：

（1）它在框架和基本概念上，与标准完全契合，同时又有非常具体实用的描述，这是标准所做不到的。每个标准由于领域划分的原因，不可能面面俱到。而著书就没有这个限制。比如风险分析，标准只是规定要进行风险分析，并不规定用什么方法去做，但在这本书里就详细介绍了当下常用的各种风险分析方法和每种方法的具体用法。这本书就像这样用非常具体实用的描述，介绍了安全工作全生命周期的每一个阶段的具体做法。

（2）本书对技术的产生及发展给予了时间上的拓展，它概略地介绍了功能安全发展的历程，使读者能够充分了解这门技术的产生背景和发展脉络。

（3）本书对技术所应用的领域也进行了拓展，除了在过程工业中的应用外，作者将技术的应用情况在核安全、机械安全方面做了比较，更有利于读者的理解。

本书融合了编者多年的工作实践经验和体会，全面系统地介绍了安全仪表系统的相关理论、方法与技术，同时注重与工程实际相结合，对于过程工业领域的工程技术人员大有裨益。

冯 晓 升

2010 年 5 月

前言

ESD、FGS，以及BMS等安全联锁或保护系统在过程工业中的应用已经有几十年的历史了。逻辑单元从最初的气动逻辑、机电继电器系统、固态（Solid-state）逻辑、可编程电子控制器（PLC），到现在的安全逻辑控制器；从故障安全（Fail Safe）设计，到诊断技术的运用，技术和安全理念都有了长足的进步。IEC61508/IEC61511等功能安全标准的发布，使得安全仪表系统在各个行业的应用有了统一的工程技术体系以及功能安全评价和管理体系。这种基于绩效（Performance-based）的工程实践，较之基于惯例（Prescriptive-based）的传统做法，可以优化改进SIS的操作性（Operability）、功能性（Functionality）、完整性（Integrity）、可靠性（Reliability），可审计性（Auditability）以及可维护性（Maintainability）。

本书循着IEC61508/IEC61511安全生命周期的脉络，以SIS在过程工业的应用为主题，解读这些功能安全标准的内涵和要求，探讨如何指导SIS的工程实践。

本书共分11章。

绪论部分对书中涉及到的一些关键概念做概括性介绍，使读者朋友初步了解本书将探讨的内容。

第2章介绍在过程工业的SIS应用中有代表性的功能安全标准，例如：德国DIN V 19250/DIN V VDE 0801、美国ANSI/ISA-84.01—1996、IEC61508，以及IEC61511，并对它们相互之间的关联和不同进行比较。

第3、4、5、6章，以及第8章，围绕着SIS的安全生命周期各阶段的活动，介绍危险和风险分析、安全保护层以及SIF的SIL确定、SIS的工程设计，以及SIS的现场安装、调试和维护。

第7章介绍SIS的核心子系统—逻辑控制器（Logic Solver）。包括SIS逻辑控制器的技术发展历程、安全系统与常规PLC的显著区别、可编程逻辑控制器的典型硬件结构和软件、可编程逻辑控制器的内部和外部通信，以及集成和验收测试等。

第9章介绍SIS的典型应用，包括以海上石油平台为例的ESD系统应用、FGS、BMS及HIPPS。展示SIS在不同应用场合的设计和系统构成。本章介绍了两个爆炸和火灾事故的案例，试图佐证SIS的技术和功能安全管理两大体系的重要性。

第10章就IEC61508/IEC61511应用中的典型问题作专题探讨。

第11章介绍IEC62061《机械安全　安全相关电气、电子和可编程电子控制系统的功能安全》，以及IEC61513《核电站　安全至关重要仪表和控制系统的一般要求》，以便读者对安全控制系统在其他行业的应用特点有所了解。

为了避免对相关定义和概念产生歧义，本书对一些重要概念加注了英文。

这本书的写作，始于2007年6月。写这本书，不论从个人的知识积累和写作文笔，都是严峻的挑战。这本书的写作并最终出版，来自于业界朋友、同事，以及家人直接或间接地

帮助和支持，借此机会，表达我对他们的敬意和感谢！

首先感谢天津市自动化学会原秘书长罗绍安先生和天津大学徐德民教授的积极鼓励，并促成了本书的写作和出版。

感谢冯晓升教授对本书写作给予的热情指导，并仔细审阅了书稿，同时欣然为本书作序。

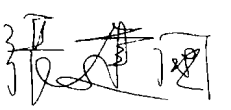
感谢全国工业过程测量和控制标准化技术委员会（SAC/TC124），石油、石化、化工、电力等行业勘察设计和生产企业，以及大学和科研院所等业界的朋友。在我的职业生涯中，他们与我分享了他们的知识和经验，拓展了我的视野。

要特别感谢荷兰 Bert Knegtering 博士的帮助，收集了本书涉及到的欧洲标准及规范。感谢 Honeywell HSMS（Honeywell Safety Management System）团队同事的帮助。不论是在安全系统 FSC/Safety Manager 的项目工程还是对 SIS 的安全咨询服务业务中，海内外的同事们，提供了很多资料，并真诚地与我分享他们的智慧、观点和经验。我无法一一列出他们的名字，但毫无疑问，他们是最终写成这本书不可或缺的支持力量。

这本书从酝酿到出版经历了四年的时间，除了时间和精力的不足，很大程度上也是因为个人能力和水平所限，不足以一气呵成地写出来，完成这本书的写作耗费了大量的业余时间和精力，我要感谢来自家庭的理解和支持。

这本书只是宽泛地讨论了 SIS 在过程工业应用中的典型问题，并没有对工程实践中具体的技术细节做深入探讨。希望本书对业界朋友理解 IEC61508/IEC61511 以及 SIS 的功能安全理念有所帮助。我的另一心愿，是将这本书奉献给大专院校工业安全、仪表、自动化等专业的同学们，希望他们对 SIS 技术领域有所关注。

本人知识和能力所限，书中会存在着错误的表述以及缺点和不足。期待着读者朋友的批评和指正。



2010 年 5 月

目 录

第1章

绪　论

在以石油/天然气开采运输、石油化工、发电、化工等为代表的过程工业领域，紧急停车系统（Emergency Shut Down System，ESD）、燃烧器管理系统（Burner Management System，BMS）、火灾和气体安全系统（Fire and Gas Safety System，FGS）、高完整性压力保护系统（High Integrity Pressure/Pipeline Protection System，HIPPS）等以安全保护和抑制减轻灾害为目的的安全仪表系统（Safety Instrumented System，SIS），已广泛应用于不同的工艺或设备防护场合，保护人员、生产设备及环境。随着自控技术和工业安全理念的发展，安全仪表系统已从传统的过程控制概念脱颖而出，并与基本过程控制系统（Basic Process Control System，BPCS），（如DCS）并驾齐驱，成为自控领域的一个重要分支。

IEC61508/IEC61511的发布，对安全控制系统在过程工业领域的应用有划时代的意义。首先，将仪表系统的各种特定应用，例如：ESD、FGS、BMS，…，都统一到SIS的概念下；其次，提出了以SIL为指针，基于绩效（Performance Based）的可靠性评估标准；再者，以安全生命周期（Safety Lifecycle）的架构，规定了各阶段的技术活动和功能安全管理活动。这样，SIS的应用形成了一套完整的体系，包括：设计理念和设计方法、仪表设备选型准入原则（基于经验使用和IEC61508符合性认证）、系统硬件配置和软件组态编程规则、系统集成、安装和调试、运行和维护，以及功能安全评估与审计等。

大体上，安全仪表系统的应用和发展，围绕着两大主题——安全功能（Safety Function）和功能安全（Functional Safety）。IEC61508/IEC61511为实现安全仪表系统的功能安全，建立了两大体系——技术体系和功能安全管理体系。

1.1　安全功能及风险降低

IEC61508将“安全功能”定义为：为了应对特定的危险事件（如灾难性的可燃性气体释放），由电气、电子、可编程电子安全相关系统，其他技术安全相关系统，或外部风险降低措施实施的功能，期望达到或保持被控设备（Equipment Under Control，EUC）处于安全状态。上述定义表明：①安全功能的执行，并不局限于电气或电子安全仪表系统，还包括其他技术（如气动、液动、机械等技术）及外部风险降低措施（如储罐的外部防护堤堰）。因此，研究安全功能要综合考虑各种技术或措施的共同影响；②安全功能是着眼于应对特定的危险事件，也就是说，安全功能有其针对性。

通常用风险的概念来评估危险事件。风险定义为危险事件发生的后果和发生可能性（或概率）的乘积。不同的危险事件，发生的后果以及发生的可能性是不同的，这就意味着，评价一个安全功能设计是否合理，首要问题是：危险事件发生的机理是否辨识清楚？是否对其

发生的风险进行了充分、准确地分析?

在现代过程工业典型的生产流程中，如果存在发生危险事件的风险，期望100%避免，不论从技术上还是从运行成本上可能都是不可行的，也是没有必要的。现实的做法，是通过分析风险的大小，依据ALARP（As Low As Reasonably Practicable）原理，即按合理的、可操作的、最低限度的风险接受原则，确定可接受的风险水平和风险降低措施。

可以看出，安全功能的作用，就是将危险事件发生的风险降低到可接受的程度，从而保证被控设备处于安全状态。因此，要设计合理有效的安全功能，必须对被控对象进行危险辨识、危险分析及风险分析。另外，不同的风险降低要求，对包括安全仪表系统在内的各种安全措施的技术形式、数量，以及力度要求，也应该是不同的。

电气、电子、可编程电子安全相关系统，其他技术安全相关系统，或外部风险降低措施在实施安全功能时，所处的位置和发挥作用的时间点是有所不同的，即处于不同的保护层(Protection Layer)。图1-1是来自IEC61508的风险降低的一般概念。

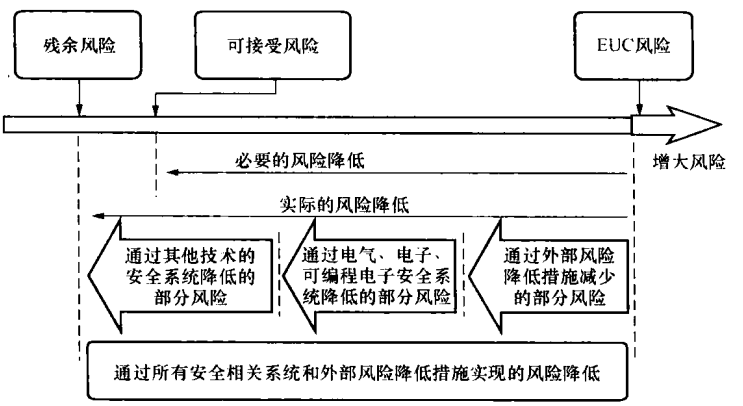


图1-1 风险降低的一般概念

要实现必要的风险降低，需要怎样的保护层？它们各自的绩效如何？相互之间具有怎样的关联性？对这些问题的分析探讨，形成了各种分析技术，如大家熟知的保护层分析（Layer Of Protection Analysis，LOPA）。

当确定了必要的风险降低要求以后，如何评价电气、电子、可编程电子安全相关系统，其他技术的安全相关系统，以及外部风险降低措施的绩效？这就引出了安全系统的另一大主题，也是IEC61508/IEC61511等标准的核心问题，即功能安全。

1.2 功能安全及安全完整性

IEC61508将功能安全定义为：与EUC和EUC控制系统有关的、整体安全的一部分，取决于电气、电子、可编程电子安全相关系统，其他技术安全相关系统和外部风险降低措施机制的正确施行。

IEC61511将功能安全定义为：与工艺过程和BPCS有关的、整体安全的一部分，取决于SIS（安全仪表系统）和其他保护层机能的正确施行。

就安全仪表系统而言，功能安全探讨的是系统本身的绩效问题，即SIS在实现其安全功

能时，能够降低风险的能力。因此，功能安全成为 SIS 设计和运行管理的核心问题之一。要达到功能安全目标，就会涉及到基本过程控制系统不曾考虑的一系列技术和管理要求。安全仪表系统与功能安全标准也正是沿着这一脉络，不断推陈出新。在过程工业中，具有里程碑意义的典型功能安全标准是德国的 DIN V 19250《控制技术　测量和控制设备应考虑的基本安全原则》/DIN V VDE0801《安全相关系统中的计算机原理》、美国的 ANSI/ISA-84.01--1996《安全仪表系统在过程工业中的应用》，以及现今大家熟知的 IEC61508《电气、电子、可编程电子安全相关系统的功能安全》和 IEC61511《过程工业领域安全仪表系统的功能安全》。

SIS 执行安全功能时的绩效或可能达到的功能安全水平，采用安全完整性（Safety Integrity）来表征。安全完整性定义为：在规定的状态和时间周期内，SIS 圆满完成所要求的安全功能的概率。

安全完整性包括硬件安全完整性（Hardware Safety Integrity），软件安全完整性（Software Safety Integrity），以及系统性安全完整性（Systematic Safety Integrity）。

（1）硬件安全完整性用于表征在危险失效模式（Dangerous Failure Mode）下，随机硬件失效（Random Hardware Failure）的可能性。随机硬件失效是指系统在正常使用状态下，在某个时间点，一个或多个元件随机出现故障（Fault），依据硬件内可能的降级机制（Degradation Mechanism），导致发生某种功能的失效。通过对系统的失效模式及其影响进行分析（Failure Modes and Effects Analysis，FMEA），借助于有效的失效率数据，可以对硬件的安全完整性进行评估计算，并且可以准确到合理的水平。另外，可以通过采用冗余结构（Redundant Architectures）设计等措施，有效提高硬件的安全完整性。

（2）软件安全完整性用于表征可编程电子系统中的软件，在规定的状态和时间周期内，实现其安全功能的可能性。

（3）系统性安全完整性用于表征在危险失效模式下系统性失效。导致系统性失效发生的典型因素包括：系统设计错误或缺陷，不当的安装、调试，不当的操作，缺乏维护管理，以及软件设计漏洞和组态缺陷等。系统性失效在很大程度上都是因为人为失误造成的，要准确地计算评估其失效率非常困难，因此，IEC61508/IEC61511 都强调在安全生命周期的架构下，通过有效的功能安全管理，来提高系统性安全完整性。

要注意必要的风险降低（参见图 1-1）和安全完整性之间的概念关联和转换。风险用于度量特定危险事件发生的后果和概率。依据设定的“可接受风险”目标，确定“必要的风险降低”要求；进一步地，依据“必要的风险降低”要求，确定安全仪表系统的安全完整性等级。

图 1-2 是 IEC61508 的风险与安全完整性概念。

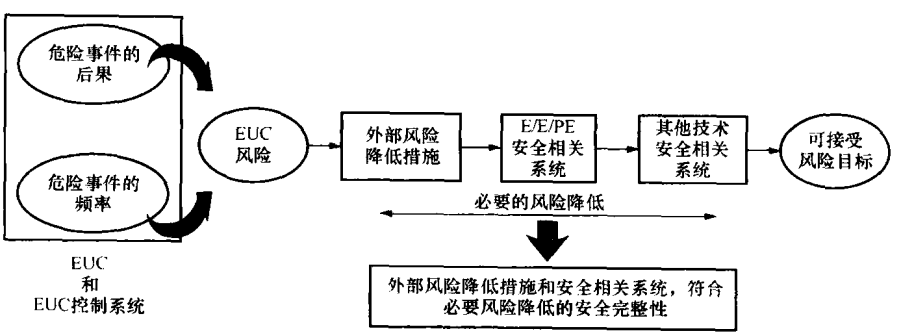


图 1-2　风险与安全完整性概念

1.3 过程工业中的风险降低机制

IEC61511-3 给出了在过程工业中典型的风险降低机制，如图 1-3 所示。

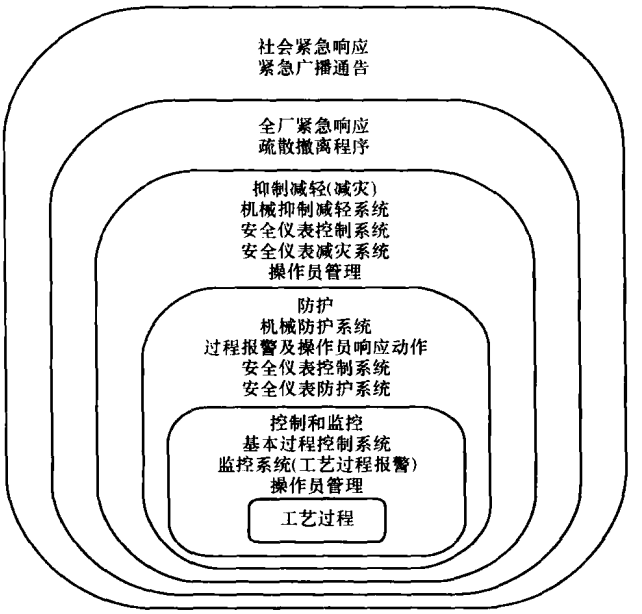


图 1-3 在过程工业中典型的风险降低机制

由图 1-3 可以看出，通过采用不同层次、不同的措施实现工艺过程的“必要风险降低”，可最终达到“可接受风险”的目标。这些不同的层次和措施，因其相互的独立性（或者说，必须保证各自的独立性），也被称为独立保护层（Independent Protection Layer，IPL），图 1-3 也常被称为保护层模型。

在工程设计中，要保证保护层的独立性、功能性、完整性、可靠性，以及可审计性。

图 1-3 中各保护层的概念理解和设计要点如下：

（1）“工艺过程”层在设计中要注重本质安全或固有安全（Inherently Safety）设计。通过工艺技术、设计方法、操作规程等有效地消除或降低过程风险，避免危险事件的发生。例如，在生产装置中改变设备的布局，改变承压或装载有危险物料容器、反应器的结构、尺寸大小；通过改进催化剂等工艺技术，避免剧烈的高温高压反应等。

（2）“控制和监控”层由基本过程控制和报警系统及操作规程构成。关注的焦点是将过程参数控制在正常的操作设定值上。

（3）“防护”层包括机械保护系统（如安全阀）及安全仪表系统—SIS。本层是 SIS 的典型应用层，如常见的 ESD 应用。它设计的出发点是降低危险事件发生的频率，保持或达到过程的安全状态。

（4）“抑制减轻（减灾）”层设计的出发点是减轻和抑制危险事件的后果，亦即降低危险事件的烈度（Severity）。典型的技术措施包括：火气（FGS）应用（火灾及燃气和有毒气体检测、报警，喷淋、水/蒸汽幕等）的 SIS 系统、防护围堰等。

（5）“全厂紧急响应”层包括消防和医疗救助响应、人员紧急撤离等机制。

（6）“社区紧急响应”层包括工厂周边社区居民的撤离、社会救助力量等机制。

1.4 SIS 与 SIF

ANSI/ISA-84.01—1996 将安全仪表系统（Safety Instrumented Systems，SIS）定义为：由传感器（Sensor）、逻辑控制器（Logic Solver）和最终控制元件（Final Control Ele-

ment）组成的系统，用于当预定的过程条件或状态出现背离时，将过程置于安全状态。其他常用的术语包括：紧急停车系统（Emergency Shutdown System，ESD 或 ESS）、安全停车系统（Safety Shutdown System，SSD），以及安全联锁系统（Safety Interlock System）。

SIS 的定义如图 1-4 所示。图中双线框内的设备为 SIS 的有机组成部分。SIS 用户接口可以包括在 SIS 中，其他接口如果对 SIS 的安全功能有潜在影响，可以将其视为 SIS 的一部分。

在 IEC61508 中，SIS 被称为安全相关系统（Safety Related System），将被控对象称为被控设备（EUC）。

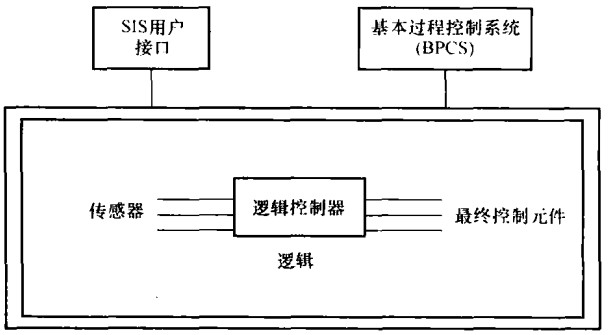


图 1-4 SIS 的定义

IEC61511 将 SIS 定义为用于执行一个或多个安全仪表功能（Safety Instrumented Function，SIF）的仪表系统。SIS 是由传感器、逻辑控制器，以及最终元件组合而成的，如图 1-5 所示。

IEC61511 又进一步指出，SIS 可以包括、也可以不包括软件。另外，当操作人员的手动操作被视为 SIS 的有机组成部分时，必须在安全要求规格书（Safety Requirement Specification，SRS）中对人员操作动作的有效性和可靠性做出明确规定，并包括在 SIS 的绩效计算中。

IEC61511 对 SIS 的定义，较之 ANSI/ISA-84.01—1996，体现了技术和理念的进步。就其共同之处而言，都是将 SIS 定义为包括传感器、逻辑控制器（或按照 Logic Solver 直译为逻辑解算器），以及最终控制元件在内的整个系统。这就意味着，任何对 SIS 的表述，都不能将其仅仅理解为逻辑控制器本身。

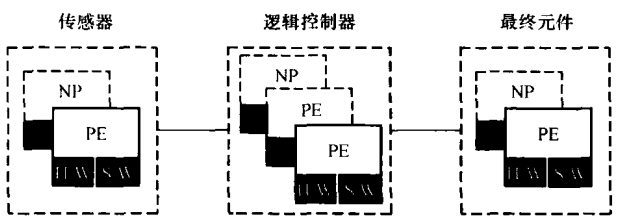


图 1-5 SIS 结构

NP—非可编程；PE—可编程电子；H/W—硬件；S/W—软件

IEC61511 提出了安全仪表功能（SIF）的概念。SIF 被定义为：由 SIS 执行的、具有特定安全完整性等级（Safety Integrity Level，SIL）的安全功能，用于应对特定的危险事件，达到或保持过程的安全状态。SIF 的特定安全完整性等级要求，是取得功能安全所必需的。安全仪表功能可以是安全仪表保护功能，也可以是安全仪表控制功能。需要说明的是，这里所说的安全仪表控制功能，是指以连续模式（Continuous Mode）操作并具有特定的 SIL，用于防止危险状态发生或者减轻其发生的后果，与常规的 PID 控制功能是完全不同的概念。

SIF，亦即由 SIS 执行的安全功能，物理结构上由传感器、逻辑控制器，以及最终元件构成，如图 1-6 所示。不过，SIF 的最根本特征是“应对特定的危险事件”并实现必要的风险降低。

SIF 是在过程危险和风险分析中辨识出来的，并根据必要的风险降低要求，确定其 SIL

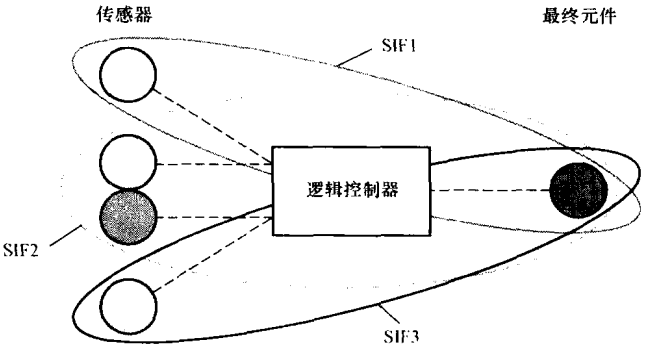


图 1-6 SIF 示例

要求。因此，SIF 是进行 SIL 评估的基础。

1.5 安全完整性等级 SIL

安全完整性反映了 SIS 执行 SIF 时，在规定的状态和时间周期内，圆满完成 SIF 的绩效能力和可靠性水平。在 ANSI/ISA-84.01—1996 中，将安全完整性等级（SIL）定义为 SIL1 到 SIL3 共三个等级，其中 SIL3 最高，SIL1 最低。

IEC61508 将 SIL 定义为四个等级，即 SIL1 到 SIL4。

IEC61511 作为 IEC61508 在过程工业领域的分支标准，保持了 SIL1 到 SIL4 的四个等级划分，不过，除了极罕见的特殊应用，在过程工业一般的应用场合，SIL3 是其最高级。在工程实践中，当过程危险和风险分析确认需要 SIL3 以上的安全完整性时，一般是将应对同一危险事件的其他技术安全系统或外部风险降低的绩效提高（参见图 1-1），从而将对 SIF 的 SIL 要求降低到 SIL3 或以下。

IEC61508/IEC61511 依据不同的操作模式，用不同的技术指标划分 SIL 等级。

IEC61511 将安全仪表功能的操作模式分为："要求操作模式"（Demand Mode of Operation）和"连续操作模式"（Continuous Mode of Operation）。

安全完整性等级对要求操作模式下的失效概率要求见表 1-1。

表 1-1　　安全完整性等级对要求操作模式下的失效概率要求

要求操作模式		
安全完整性等级（SIL）	要求时平均失效概率（PFD_{avg}）	目标风险降低
4	$\geqslant 10^{-5}$到$<10^{-4}$	>10，000 到≤100，000
3	$\geqslant 10^{-4}$到$<10^{-3}$	>1000 到≤10，000
2	$\geqslant 10^{-3}$到$<10^{-2}$	>100 到≤1000
1	$\geqslant 10^{-2}$到$<10^{-1}$	>10 到≤100

SIF 的要求操作模式指的是，在响应过程状态或其他"要求"（Demand）时，执行特定的动作（如关闭阀门）。要求操作模式的特征，是当 SIF 出现危险失效，并且"要求"出现时，才会导致潜在危险发生。典型的"要求"包括：工艺过程参数出现异常，达到设定的安

全极限值，或者 BPCS 本身处于失效状态。这就意味着 SIF 的危险失效，并不一定即刻导致危险。常见的 ESD 应用就是典型的要求操作模式。这是因为当 ESD 出现危险失效（例如，对于失电关停的联锁系统，当 DO 输出电路出现故障，不能对停车要求进行响应）时，如果工艺状态没有达到联锁设定值，或者 DCS 运行正常并将工艺参数控制在正常给定值上，并不会马上造成危险。

从表 1-1 可以看出：每个 SIL 等级对应着 SIF 一个数量级的平均失效的概率，它用符号表示为 PFD_{avg}；目标风险降低数值，也称为风险降低因数 RRF（Risk Reduction Factor）。PFD_{avg} 与 RRF 互为倒数，即 $PFD_{avg}=1/RRF$。它们的物理含义是，每提升一个 SIL 等级，意味着 SIF 的平均失效概率降低一个数量级，也意味着将危险事件发生的可能性降低 10 倍。

安全完整性等级对连续操作模式下 SIF 的危险失效频率要求见表 1-2。

SIF 的连续操作模式指的是，当 SIF 出现危险失效时，潜在的危险将会立即发生，除非存在其他防止措施。连续模式涵盖执行连续安全控制，以便保持功能安全的安全仪表功能。

安全完整性等级的数量划分，为工程设计和 SIS 设备选型提供了基准。

在工程实践中，采用一些较低 SIL 的系统，配置成较高 SIL 要求的 SIF 是可能的。例如，将一个 SIL2 和一个 SIL1 的系统并联在一起，可满足 SIL3 功能的要求。

表 1-2 安全完整性等级对连续操作模式下 SIF 的危险失效频率要求

连续操作模式	
安全完整性等级（SIL）	完成安全仪表功能危险失效的目标频率（每小时）
4	$\geqslant 10^{-9}$ 到 $<10^{-8}$
3	$\geqslant 10^{-8}$ 到 $<10^{-7}$
2	$\geqslant 10^{-7}$ 到 $<10^{-6}$
1	$\geqslant 10^{-6}$ 到 $<10^{-5}$

1.6 SIS 中逻辑控制器的技术特征和典型结构

SIS 中的逻辑控制器是由电气、电子、可编程电子技术构成的逻辑运算处理设备。根据不同的应用、技术、年代，逻辑控制器可能是：机电继电器、固态逻辑、可编程电子系统、马达驱动计时器（Timer）、固态继电器和计时器、硬接线逻辑，以及上述技术的组合。

需要注意的是，功能安全标准并未对采用的具体技术进行限定，而是通过对逻辑控制器以及传感器和最终控制元件的功能安全要求，来规范系统设计和应用。

以 PLC 为代表的可编程电子系统的出现，为大规模的自动保护逻辑的编程应用以及修改提供了便利。但是，随着系统的复杂，人们对其失效状态的预期和掌控，较之简单传统的设备，如机电继电器或固态逻辑控制器，变得十分困难。因此，对于现代基于计算机技术的可编程电子系统或仪表设备在安全保护中的应用，功能安全成为突出问题。

安全逻辑控制器的出现，为关键控制和安全保护的应用提供了可靠的技术保证。在许多文献中，将传统的 PLC 称为常规 PLC（Conventional PLC），而将安全逻辑控制器系统称为安全 PLC（Safety PLC）。

安全逻辑控制器，尽管也像常规 PLC 那样完成逻辑和数学运算，有输入输出卡件作为接收传感器输入信号和到最终执行元件输出信号的接口，有与其他控制设备的通信接口，以及人机界面等，但在研发的安全理念上，与常规 PLC 截然不同。

安全逻辑控制器在技术上的显著特点是：系统必须有极高的可靠性，通过冗余等措施避免整个系统的功能失效；如果出现某种失效状态，它必须是以可预见的、安全的方式出现。它强调内部诊断，通过硬件和软件的有机结合，对检测出系统内部的异常运行状态，做出针对性的处理，如报警、隔离、切除，甚至安全关停；在系统研发时，采用失效模式、影响和诊断分析（Failure Modes，Effects and Diagnostic Analysis，FMEDA）技术，确定系统中的每个部件将会出现怎样的失效，以及系统如何检测、应对这些失效，保证能够检测出99%以上的内部元器件潜在的危险失效；要采用一系列的专门技术确保软件的可靠性，并保证通过其数字通信端口进行读写操作的私密安全（Security）。

安全逻辑控制器与常规 PLC 的不同，还体现在必须通过第三方的权威认证，例如，德国 TÜV 的认证，以便满足国际功能安全标准严格的安全和可靠性要求。

当今世界主流的安全逻辑控制器，或者采用以硬件冗余和故障容错（Fault Tolerant）为基础的“表决”（Voting）技术，如 2oo3（2 out of3）；或者采用基于诊断（Diagnostic）的技术，如 1oo1D、1oo2D，以及 2oo4D（QMR）等。

2oo3 表决结构，采用三套控制器，并将其输出组合连接成“表决”电路，最终的输出，取决于表决结果的“多数（Majority）”，当其中的至少两套输出导通时，其最终的输出是得电的（Energized）；当其中的至少两套输出切断时，其最终的输出是失电的（De-energized）。

进一步分析 2oo3 结构的表决电路可以看出，单一的失效模式：危险（短路）或安全（开路），系统都是可容忍的（Tolerated）。当其中的一套控制器的输出出现开路故障时，整个系统将降级到 1oo2 结构模式；当其中的一套控制器的输出出现短路故障时，整个系统将降级到 2oo2 结构模式；这两种情形都不会影响其安全操作。只有当其中的两套同时出现危险（短路）故障时，整个系统将处于危险失效状态。

诊断技术的控制器结构，是在系统中嵌装诊断电路，当诊断到输出出现危险故障（短路）时，该诊断电路可直接切断其输出。常见的诊断是“看门狗”（Watchdog）或称“心跳”（Heartbeat）的技术。它通过对输出电路加载测试脉冲，检验其回讯，实时诊断其状态。因为其诊断是基于系统内的标准特征值，所以可配置成 1oo1D 单通道的结构。当构成冗余的系统（如 1oo2D）时，通过比较诊断技术（Comparison Diagnostic Technique）对两套控制器的状态进行实时比较，以便检测它们互相之间是否一致。这种比较提供了另一层诊断。

典型的逻辑控制器结构总汇见表 1-3（资料来源：Exida）。

表 1-3　　典型的逻辑控制器结构总汇

正常操作模式	一次降级 (1st Degradation)	二次降级 (2nd Degradation)	安全完整性 (Safety Integrity)	故障容错 (Fault Tolerence)	备　注
1oo1	关停（Shutdown）		低	低	
1oo2	关停（Shutdown）		高	低	
1oo3	关停（Shutdown）		高	低	
2oo2	关停（Shutdown）	关停（Shutdown）	低	高	
2oo3	1oo2	关停（Shutdown）	高	高	一些供应商声称其系统降级模式可有三次降级，第三次为有时间限制的 1oo1

续表

正常操作模式	一次降级 (1st Degradation)	二次降级 (2nd Degradation)	安全完整性 (Safety Integrity)	故障容错 (Fault Tolerence)	备 注
1oo2D	1oo1D	关停 (Shutdown)	高	高	1oo2D 中的 "D (诊断)" 标志着系统能力从 2oo2 提升到 1oo2；要保证诊断电路输出触点的动作是独立的
2oo4D (仅指 CPU)	1oo2D (仅指 CPU)	关停 (Shutdown)	高	高	这种结构仅 CPU 是 2oo4 表决，I/O 必须是 1oo2D 的结构才能取得高的故障裕度

1.7 SIF 子系统的结构约束

SIF 是由传感器、逻辑控制器，以及最终执行元件组成的，其 SIL 等级除了应符合 PFD_{avg} 计算值外，它所能达到的最大硬件安全完整性等级，受限于这些子系统（传感器、逻辑控制器，以及最终元件）相应的最低硬件故障裕度（Hardware Fault Tolerance，HFT）要求。也就是说，不论其声称的可靠性多高，从硬件结构上限制了所能达到的 SIL，这就是 IEC61508 中提出的结构约束（Architectural Constraints）。

子系统的硬件故障裕度为 N，表示当该子系统存在 $N+1$ 个故障时，将会导致其安全功能的丧失。在确定硬件故障裕度时，并不考虑是否有控制该故障影响的其他措施，例如诊断（不过，诊断能力影响安全失效分数）。另外，当一个故障直接导致一个或多个后续故障时，这些后果要视为是同一个单一故障。

IEC61508 将子系统划分为 A 型和 B 型两种。

同时满足以下条件者为 A 型子系统：

1）所有组成部件的失效模式都能被完美地定义。

2）在故障状态下，子系统的行为能够完全确定。

3）有来自现场经验的足够可靠的失效数据，佐证所声称的检测出的和未检测出的危险失效率是真实有效的。

符合以下任一条件者为 B 型子系统：

1）至少一个组成部件的失效模式不能被完美地定义。

2）故障状态下的子系统行为不能完全被确定。

3）没有来自现场经验的足够可信的失效数据，佐证所声称的检测出的和未检测出的危险失效率是真实有效的。

很显然，A 型子系统是常见的简单仪表设备，如开关、继电器、阀门等。而逻辑控制器、智能变送器等，是典型的 B 型子系统。

A 型和 B 型子系统的结构约束如下。