

ICS 75.020

E 09

备案号: 11646—2003

标准分享网  
www.bzfxw.com

**SY**

# 中华人民共和国石油天然气行业标准

SY/T 10045—2003

---

## 工业生产过程中安全仪表系统的应用

Application of safety instrumented systems for the process industries

2003 - 03 - 18 发布

2003 - 08 - 01 实施

---

国家经济贸易委员会      发 布

## 目 次

前言 .....	III
ANSI/ISA 前言 .....	IV
引言 .....	V
1 范围 .....	1
1.1 安全仪表系统 (SIS) 的范围 .....	1
1.2 不包括部分 .....	1
2 符合标准 .....	2
2.1 符合性指导 .....	2
2.2 现有的系统 .....	2
3 术语定义和缩写 .....	2
3.1 术语定义 .....	2
3.2 缩写 .....	8
4 安全生命周期 .....	8
4.1 范围 .....	8
4.2 安全生命周期步骤 .....	9
5 编制安全要求规格书 .....	10
5.1 目的 .....	11
5.2 输入要求 .....	11
5.3 安全功能要求 .....	11
5.4 安全完整性要求 .....	11
6 SIS 概念设计 .....	11
6.1 目的 .....	11
6.2 概念设计要求 .....	11
7 SIS 详细设计 .....	12
7.1 目的 .....	12
7.2 一般要求 .....	12
7.3 SIS 逻辑控制器 .....	12
7.4 现场设备 .....	13
7.5 接口 .....	13
7.6 电源 .....	14
7.7 系统环境 .....	14
7.8 应用逻辑要求 .....	15
7.9 维护或测试设计要求 .....	15
8 安装、调试和预启动认可试验 .....	15
8.1 目的 .....	15
8.2 安装 .....	15
8.3 调试 .....	15
8.4 预启动认可试验 (PSAT) .....	16

9 SIS 操作和维护 .....	16
9.1 目的 .....	16
9.2 培训 .....	16
9.3 文件 .....	16
9.4 SIS 操作程序 .....	16
9.5 维护程序 .....	17
9.6 测试、检验和维护 .....	17
9.7 功能试验 .....	17
9.8 功能测试文件编制 .....	18
10 SIS 变更管理 (MOC) .....	18
10.1 目的 .....	18
10.2 变更管理 (MOC) 程序 .....	18
10.3 变更管理文件 .....	19
11 停运 .....	19
11.1 目的 .....	19
11.2 通则 .....	19
12 差异 .....	19
12.1 术语差异 .....	19
12.2 组织差异 .....	20
12.3 技术差异 .....	22
附录 A (资料性附录) 决定安全仪表系统 (SIS) 安全完整性级别 (SIL) 示例 .....	23
附录 B (资料性附录) SIS 设计需要考虑的问题 .....	28
附录 C (资料性附录) 参考资料 .....	46
附录 D (资料性附录) 举例 .....	49

## 前 言

为适应海上油气资源开发生产发展的需要，中国海洋石油总公司等采用美国国家标准化组织（ANSI）和美国仪表学会（ISA）的标准《工业生产过程中安全仪表系统的应用》1996年版（ANSI/ISA S84.01—1996 Application of safety instrumented systems for the process industries），作为中华人民共和国石油天然气行业标准发布。

本标准在石油天然气开发工程设计、建造的使用中，如遇到涉及原标准所在国政府或其他主管当局的法令、法规和规定时，一律按中华人民共和国政府或政府主管部门颁布的相应法令、法规和规定执行。

本标准的计量单位均以国家已颁布的法定计量单位为准。

本标准的附录 A、附录 B、附录 C 和附录 D 都是资料性附录。

本标准由海洋石油工程专业标准化技术委员会提出并归口。

本标准起草单位：中海石油研究中心开发设计院。

本标准主要起草人：俞曼丽、周学军、屈长龙。

本标准主审人：洪毅。

## ANSI/ISA 前言

本前言及所有脚注、附录及草案技术报告 84.02 (ISA-dTR84.02) 作为资料参考, 不作为 ANSI/ISA-S84.01—1996 的标准部分。ISA-S84.01 出版时, ISA-dTR84.02 还在编制。资料查询, 与 ISA 联系。

本标准是国际测量和控制学会 ISA 服务的部分, 目的是致力于仪表领域的统一性。为了具有实际意义, 本标准不应静止不变, 应进行周期性的复审。为达到此目标, 学会欢迎提出建议和批评, 并请函告 ISA 标准和准则委员会秘书, 地址是: 67Alexander Drive; P.O.Box 12277; Research Triangle Park, NC 27709; 电话: (919) 549—8401; 传真: (919) 549—8288; 电子邮件: standards@isa.org。

ISA 标准和准则部意识到在准备仪表标准、推荐作法和技术报告时, 米制单位增长的需要, 特别是国际单位制 (SI), 更意识到美国用户在处理与其他国家的商业和专业事务时, ISA 标准中将有关参考并入 SI 制 (和米制) 带来的好处。为此, 本部门将尽力在所有新编和修订版标准中尽可能在最大范围引进 SI 制和可接受的米制单位。由电子和电气工程师协会出版的 ANSI/IEEE Std 268—1992《米制应用指南》及更新版将作为定义、符号、缩写和转换系数的参考指南。

ISA 的政策是鼓励和欢迎所有有关的个人和有兴趣者参与 ISA 标准的编制。个人在 ISA 标准编制过程中的参与决不构成该个人的雇主、ISA、任何 ISA 的标准、推荐做法和技术报告的认可。

S84.01 编制的目的是最终成为国际电工委员会 (IEC) 正在编制的标准的一部分。因而, 本标准的格式和结构与以往的 ISA 标准有些不同, 所提供的背景资料可以帮助读者更好地理解 S84.01 的主要内容。

IEC 已委托编制一套包含所有工业领域安全系统所有方面的国际标准, 标准名称是《功能性安全: 安全有关的系统》, 在 IEC 第 65 技术委员会、65A 分委员会、第 10 工作组指导下工作, 标准为 IEC 草案出版物 1508, 现正在编制过程中, 分为七个部分:

- 第 1 部分 一般要求
- 第 2 部分 电气/电子/可编程电子系统 (E/E/PES) 要求
- 第 3 部分 软件要求
- 第 4 部分 定义和术语缩写
- 第 5 部分 第 1 部分应用指南
- 第 6 部分 第 2 部分、第 3 部分应用指南
- 第 7 部分 技术和方法参考书目

该标准工作内容是定义所有工业的共同要求, IEC 意在编制另外的标准, 反映不同工业部门 (如核、制药、航空、工业生产过程等) 的特殊要求。

IEC 已委托了一个分会 IEC1511 来编制关于工业生产过程安全仪表系统应用的特殊工业国际标准。ISA-S84.01—1995 编写目的是为用作该特殊标准的基础。S84.01 的结构、格式和内容是在此情况下编写的。S84.01 与 IEC 草案出版物 1508—1995 有很大的不同, 如第 12 章所述。S84.01 出版时, IEC 草案出版物 1508 尚在编制, 因此, ISA S84 将继续支持和跟踪 IEC 草案出版物 1508 的编制, 当 IEC 草案出版物 1508 出版时, 根据需要, 将修改 S84.01。

IEC 编写指南已用来帮助本标准与正在编制的 IEC 草案出版物 1508 的总标准和其他部门特殊标准保持一致。

本标准由 ISA 标准和准则委员会 1996 年 2 月 15 日批准出版。

## 引 言

### 一、用途

本标准阐述工业生产过程中安全仪表系统（SIS）的应用。安全仪表系统包括电气（E）、电子（E）及可编程电子（PE）技术。本标准包括在国际电工委员会（IEC）草案出版物 1508 的框架内（参考 C.8 和参考 C.9），专用于工业生产过程。本标准符合后面提到的安全生命周期（见图 4.1）。

本标准为下述从事安全仪表系统的人员编写：

1. 从事设计、生产、选择及应用安全仪表系统产品的人员；
2. 从事安装、调试及预启动认可试验的人员；
3. 从事操作、维修、文件编制及测试的人员。

### 二、目的

定义安全仪表系统的要求。

### 三、构成

本标准由三个主要部分组成，第 1 章至第 11 章为标准的主体部分，介绍强制性的要求，第 12 章列出 ISA-S84.01 和 IEC 草案出版物 IEC 1508 之间的主要不同点，附录 A 至附录 D 介绍在安全仪表系统应用中具有价值的非强制性的技术信息。

草案技术报告 84.02（ISA-dTR84.02）不包括在本标准中，另行发布，它将提供安全完整性级别分析中非强制性（参考性）的技术指导。

# 工业生产过程中安全仪表系统的应用

## 1 范围

注：本章是本标准的主体部分，是强制性的要求。

本标准阐述了用于工业生产过程中自动化安全仪表系统中的电气/电子/可编程电子系统（E/E/PES）、传感器、终端元件及接口要求（参考 C.6）。应用 E/E/PES 技术的例子有：

- a) 机电继电器；
- b) 固态逻辑；
- c) 可编程电子系统；
- d) 马达驱动的定时器；
- e) 固态继电器及定时器；
- f) 硬线逻辑；
- g) 上述组合。

### 1.1 安全仪表系统（SIS）的范围

1.1.1 图 1.1 定义安全仪表系统的范围及可能包括在系统中的设备。本标准阐述的安全仪表系统在双线范围内。

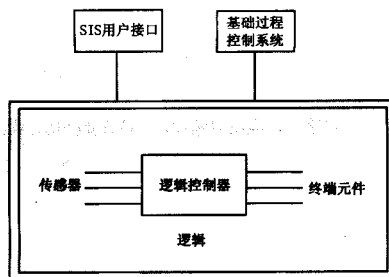


图 1.1 安全仪表系统（SIS）定义

1.1.2 安全仪表系统包括从传感器到终端元件的所有元件，包括输入、输出、电源、逻辑控制器。安全仪表系统用户接口可以包括在安全仪表系统中。

1.1.3 其他与安全仪表系统的接口，如果可能影响其安全功能，则认为是在安全仪表系统的范围内。

### 1.2 不包括部分

1.2.1 本标准确定安全生命周期（见图 4.1）中的所有步骤，但不定义某些步骤中的可能使用的方法。

1.2.2 本标准不涉及非安全仪表系统部分设计管理及过程启动管理。

1.2.3 如果政府主管部门已经建立了过程安全设计、过程安全管理或其他要求，这些法律在所有情况下比本标准的要求更具有优先权。这些因素必须以适当的步骤融入安全生命周期。

1.2.4 本标准不涉及只用于核工业的规范、规则或其他要求。

1.2.5 本标准不包括应用过程危险分析方法确定过程危险的活动。

- 1.2.6 本标准不规定何处需要使用安全仪表系统。
- 1.2.7 本标准不用作独立的系统采办文件，不排除使用合理的工程判断，也不强制使用任何特定的技术。
- 1.2.8 本标准不适用于基础过程控制系统（BPCS）。
- 1.2.9 本标准不适用于气动或液压逻辑控制器。
- 1.2.10 本标准不考虑使用目前未在安全仪表系统中使用的技术。当有新技术产生并被认可后（如 ISA SP50 现场总线），将在本标准修订版中（5 年 1 次）体现。在这期间，如果证明新系统性能优越，新技术在用于安全系统前应得到用户的批准。在这些情况下，新技术可能不符合 S84.01 的一些标准要求，例外部分应编制文件证明新方法满足安全要求。
- 1.2.11 操作人机界面信息的人员的能力分析是过程危险分析的一部分，不在本标准的范围内。
- 1.2.12 监视慢性健康状况的检测仪表不在本标准范围内。
- 1.2.13 本标准不包括主要为了财产保护目的而安装的仪表。
- 1.2.14 操作员动作是将工艺过程恢复到安全状态的惟一手段的系统（如报警系统、火气探测系统）不在本标准范围内。

## 2 符合标准

注：本章是本标准的主体部分，是强制性的要求。

为了符合本标准，应遵循下列要求。

### 2.1 符合性指导

- 2.1.1 必须说明每一项要求已得到满足，符合标准，从而达到本章的目的。
- 2.1.2 通过参考资料性附录，要求能够满足时，表明一系列的技术及方法可以用于满足要求，包括附录中没有列出的技术和方法。
- 2.1.3 在安全仪表系统设计时，采用包括在第 1 章至第 11 章的技术和方法被认为是好的工程惯例。
- 2.2 现有的系统
- 2.2.1 在本标准出版以前，根据规范、标准或惯例设计、施工的 SIS，业主/作业者须确定设备的设计、维护、检验、试验及运转符合安全要求。

## 3 术语定义和缩写

注：本章是本标准的主体部分，是强制性的要求。

### 3.1 术语定义

为实现本标准的意图将使用到下列术语。

#### 3.1.1

**应用程序 application program**

见软件（3.1.58.1）。

#### 3.1.2

**应用软件 application software**

见软件（3.1.58.1）。

#### 3.1.3

**结构 architecture**

组成 SIS 的硬件或模块的排列及连接。

#### 3.1.4

**可用性 availability**

见安全可用性（3.1.51）。



## 3.1.5

**基础过程控制系统 Basic process control system (BPCS)**

对来自控制设备和（或）操作员的输入信号进行响应并产生输出信号，使控制设备按所设定的方式运行的系统。例如，放热反应的控制、压缩机的防喘振控制、加热炉的燃料/空气的控制。也称做过程控制系统。

## 3.1.6

**旁路 bypassing**

使 SIS 的安全功能暂时失效的动作。

## 3.1.7

**公共原因 common cause**

## 3.1.7.1

**公共原因故障 common cause fault**

引起一系统中多个元件故障的单一源。单一源可以来自系统的内部或外部。

## 3.1.7.2

**公共原因失效 common cause failure**

公共原因故障结果。

## 3.1.8

**通信 communication**

## 3.1.8.1

**外部通信 external communication**

SIS 与 SIS 之外的各系统或设备之间的数据交换，包括共同享有的操作员界面、维护/工程师界面、数据采集系统、上位机等在内。

## 3.1.8.2

**内部通信 internal communication**

给定的 SIS 范围内各装置之间的数据交换。包括就地或远程 I/O 总线、总线底板连接等。

## 3.1.9

**覆盖率 coverage**

见诊断覆盖率 (3.1.14)。

## 3.1.10

**隐性故障 covert fault**

隐藏的、隐蔽的、未被发现的、潜在的故障等。

## 3.1.11

**停运 decommissioning**

将完整的 SIS 从运行装置中永久拆除。

## 3.1.12

**失电跳闸 de-energize to trip**

SIS 电路的输出及设备在正常情况下带电，失去动力源（如电源，气源）引起跳闸动作。

## 3.1.13

**要求 demand**

需要 SIS 采取适当的行动防止危险的事件发生，或者减轻危险事件后果的条件或事件。

## 3.1.14

**诊断覆盖率 diagnostic coverage**

SIS 实时故障检测能力，检测到的故障与全部故障的比率。

3.1.15

不同 diverse

为了减少公共原因故障，使用不同的技术、设备或设计方法实现执行相同功能（参见 3.1.45, 3.1.55 和 B.2）。

3.1.16

电气/电子/可编程电子系统 E/E/PES [electrical (E) /electronic (E) /programmable electronic systems (PES)]

本标准中电气指用机电技术实现逻辑功能（例如，机电继电器、电驱动定时器）；电子指用电子技术实现逻辑功能（例如，固态逻辑、固态继电器等）；可编程电子系统指可编程或可组态设备完成逻辑功能 [例如，可编程逻辑控制器 (PLC)、单回路数字控制器 (SLDC) 等]，现场设备不包括在 E/E/PES 内。

3.1.17

电子 electronic (E)

参见 E/E/PES (3.1.16)。

3.1.18

内置软件 embedded software

见软件 (3.1.58.2)。

3.1.19

得电跳闸 energize to trip

SIS 电路的输出在正常情况下不带电，加上动力源（如电源、气源）引起跳闸动作。

3.1.20

故障安全 fail-safe

故障情况下，能够进入预定安全状态的能力。

3.1.21

容错 fault tolerance

系统能够在少量硬件和软件故障时继续正确执行其设定功能的能力。

3.1.22

现场设备 field devices

连接到 SIS I/O 现场端子上的设备。现场设备包括现场接线、传感器、终端控制元件、通过硬线连至 SIS I/O 端子的操作员界面设备等。

3.1.23

固件 firmware

操作可编程电子而需要将软件内置在被保护的存储器中的特殊存储器单元。

3.1.24

强制 forcing

一种 PES 工程师站功能，可以不执行应用程序，而改变输入和输出的状态。

3.1.25

功能试验 functional testing

根据安全要求规格书周期性检查 SIS 操作。

3.1.26

硬件构造 hardware configuration

见结构 (3.1.3)。

3.1.27

**硬线 hard-wired**

不用软件或固件而完成的电气连接。

**3.1.28**

**危险 hazard**

对人员或环境可能造成危害的化学或物理状态（参考 C.12）。

**3.1.29**

**输入/输出模块 input/output modules**

**3.1.29.1**

**输入模块 input module**

在 E/E/PES 或子系统中，用作外部设备的接口，将输入信号转换成 E/E/PES 可以使用的信号。

**3.1.29.2**

**输出模块 output module**

在 E/E/PES 或子系统中，用作外部设备的接口，将输出信号转换成可以驱动外部设备的信号。

**3.1.30**

**接口 interface**

转换信号的共享边界。

**3.1.31**

**集成 integration**

将多个元件或子系统组合形成一个系统的过程。

**3.1.32**

**逻辑控制器 logic solver**

执行应用逻辑的 E/E/PES 元件或子系统。电子或可编程电子系统中包括输入/输出模块。

**3.1.33**

**离线关断 off-line**

与 SIS 连接的过程被关断。

**3.1.34**

**在线运行 on-line**

与 SIS 连接的过程在运行。

**3.1.35**

**显性故障 overt faults**

被发现的、被检测到的故障。

**3.1.36**

**许可 permissive**

执行下一阶段前必须满足的逻辑顺序条件。

**3.1.37**

**预启动认可试验 pre-startup acceptance test (PSAT)**

确认全套 SIS 的性能满足安全要求规格书及设计的过程。

**3.1.38**

**预防维护 preventive maintenance**

根据厂商的推荐做法或根据积累的操作经验，以固定的时间表对设备进行维护。

**3.1.39**

**期望故障率 probability of failure on demand (PFD)**

指示系统停止响应指令的概率值。系统在一定时间间隔内停止响应指令的平均概率称做平均故障

率 (PFDavg)。PFD 等于 1 减去安全可用性 [见安全可用性 (3.1.51)]。

**3.1.40**

**工业生产过程部门 process industry sector**

包括但不限于下列过程：生产、加工、制造和（或）油气处理、木材、金属、食品、塑料、石油化学制品、化工、蒸汽、电力、医药、废料。

**3.1.41**

**可编程电子系统 programmable electronic system (PES)**

见 E/E/PES (3.1.16)。

**3.1.42**

**保护层 protection layer**

设计的安全特性或保护系统或保护层，通常包括特殊过程设计、处理设备、管理步骤、基础过程控制系统 (BPCS) 和（或）对逼近危险有计划的做出保护反应，反应可以是自动或手动启动（参见附录 A）。

**3.1.43**

**定性的方法 qualitative methods**

运用经验或良好的工程判断进行设计和评价的方法。

**3.1.44**

**定量的方法 quantitative methods**

根据数据和数学分析进行设计和评价的方法。

**3.1.45**

**冗余 redundancy**

使用多个元件或系统完成同样的功能。冗余可以用相同元件（相同冗余）或不同元件（不同冗余）实现。

**3.1.46**

**可靠性 reliability**

系统在规定条件下，一定时间内完成规定功能的概率。

**3.1.47**

**替换 replacement in kind**

满足设计说明的替换。

**3.1.48**

**复位 reset**

控制设备回到事先设定的正常的操作状态。

**3.1.49**

**风险评估 risk assessment**

进行风险评估并用结果做决定的过程。

**3.1.50**

**安全状态 safe state**

受控设备或过程应处于过程危险分析 (PHA) 定义的状态。

**3.1.51**

**安全可用性 safety availability**

运行过程中，安全系统能够完成其指定安全功能的时间比。在本标准中，平均故障率 (PFDavg) 是常用的术语。(PFD 等于 1 减去安全可用性，见 3.1.39)。

**3.1.52**

**安全完整性级别 safety integrity level (SIL)**

安全仪表系统中，安全完整性级别分为 3 种。安全完整性级别按照故障率（PFD）定义，如表 3.1。

**表 3.1 安全完整性级别 (SIL)**

安全完整性级别	平均故障率范围
1	$10^{-1} \sim 10^{-2}$
2	$10^{-2} \sim 10^{-3}$
3	$10^{-3} \sim 10^{-4}$

**3.1.53****安全仪表系统 safety instrumented systems (SIS)**

由传感器、逻辑控制器及终端元件组成的系统，其目的是出现故障时，将过程处于安全状态（见图 1.1）。使用的其他术语包括紧急关断系统（ESD，ESS）、安全关断系统（SSD）及安全联锁系统。

**3.1.54****安全生命周期 safety life cycle**

安全仪表系统完成从概念设计到停运的全过程（见图 4.1）。

**3.1.55****分离 separation**

使用多个设备或系统将控制与安全功能分开。分离可用相同元件（相同分离）或不同元件（不同分离）实现。

**3.1.56****应该 shall**

指强制性要求。

**3.1.57****SIS 元件 SIS components**

组成 SIS 的元件。SIS 的元件如现场设备、输入模块、输出模块及逻辑控制器。

**3.1.58****软件 software****3.1.58.1****应用软件 application software**

用户专用的，PES 中满足安全要求规格书的 SIS 功能描述程序软件（见第 5 章）。通常，应用软件包括逻辑顺序、许可、界限、表达式等，控制输入、输出、计算、必要决定，从而满足安全功能要求。

**3.1.58.2****内置软件 embedded software**

厂商提供的系统软件，用户不能修改。内置软件也称做固件或系统软件。

**3.1.58.3****公用软件 utility software**

用于建立、维护、管理应用程序的软件工具。运行 SIS 无需这些软件工具。

**3.1.59****谬误跳闸 spurious trip**

指过程关断不是由 SIS 设计保护的过程故障引起的跳闸（如，由于硬件故障、软件故障、电气故

障、瞬变、接地干扰等引起的故障)，也称做噪扰跳闸和假关断。

### 3.1.60

**系统故障 systematic failures**

在特定输入组合或特定环境条件下，安全生命周期中由于过失（包括错误和动作疏忽）引起的SIS故障。系统故障可能发生在安全生命周期中的任何一步。

### 3.1.61

**试验间隔 test interval (TI)**

功能试验时间间隔。

### 3.1.62

**用户批准的 user approved**

用户已评估过的，并确定可应用的硬件、软件、程序等。

### 3.1.63

**确认 verification**

确认安全生命周期中特定步骤目标满足的过程。

### 3.1.64

**表决系统 voting system**

冗余系统（如， $n$ 选 $m$ ，2选1，3选2等）中，需要 $n$ 中至少有 $m$ 个相同，SIS才能动作。

## 3.2 缩写

BPCS：基础过程控制系统

CFR：联邦法规

E/E/PES：电气/电子/可编程电子系统

I/O：输入/输出

MOC：变更管理

MTBF：平均故障间隔时间

MTTF：平均无故障时间

MTTR：平均修复时间

OSHA：职业安全健康署

PES：可编程电子系统

PF：故障率

PHA：过程危险分析

PSAT：预启动认可试验

PSSR：预启动安全检查

SIL：安全完整性级别

SIS：安全仪表系统

WDT：监视定时器

## 4 安全生命周期

注：本章是本标准的主体部分，是强制性的要求。

### 4.1 范围

**4.1.1** 本章根据安全生命周期编排（见图4.1）。安全生命周期包括安全仪表系统（SIS）从概念设计到停运全过程的活动。本章不包括实现安全生命周期前面部分的方法，如：

- a) 进行过程概念设计；
- b) 进行过程危险分析及风险评估；

- c) 定义非 SIS 保护层;
  - d) 定义对一个 SIS 的需求;
  - e) 决定需要的安全完整性级别。
- 这些内容不包括在本章范围内。

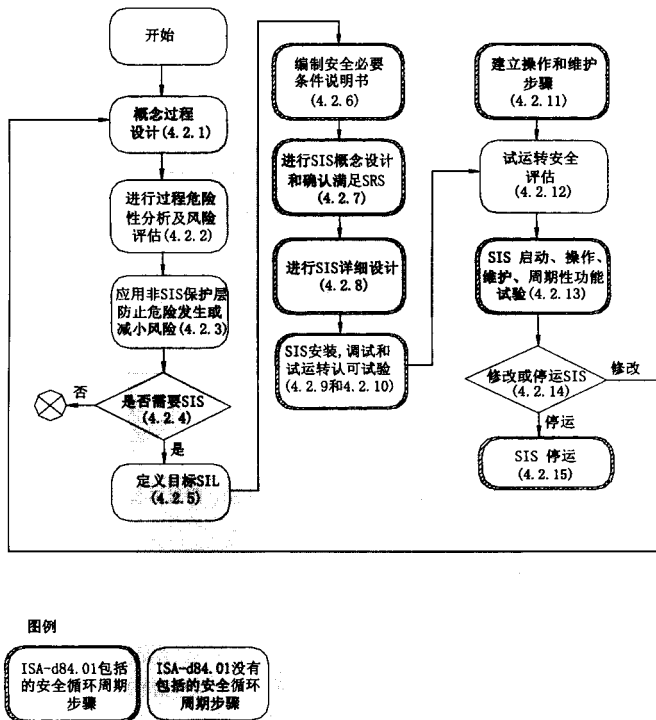


图 4.1 安全生命周期

在 SIS 安全生命周期中,有的地方可能需要反复。在给出的安全生命周期中只标出了几个地方,但这并不表示只有这些地方需要反复。

## 4.2 安全生命周期步骤

4.2.1 安全生命周期的第一步是进行过程概念设计,完成此步骤的方法不在本章范围内。

4.2.2 第二步是确定过程的危险事件及评估风险级别。本标准不阐述进行分析及评估的方法,但是在应用本标准前,假定已进行过分析及评估。完成此步骤的方法不在本章范围内。

4.2.3 在一旦确定了危险及风险,采用适当的技术(包括修改过程或设备)来减小危险、减轻危害结果或减小危险发生的可能性。第三步包括将非 SIS 保护层应用到过程系统。完成此步骤的方法不在本章范围内。

#### 4.2.4 下一步评估是确定是否提供了足够数量的非 SIS 保护层。

如果提供了足够数量的非 SIS 保护层，则可以不用 SIS 保护层。因而，在考虑加上 SIS 保护层以前，宜先考虑应用非 SIS 保护技术改变过程和（或）设备。完成此步骤的方法不在本章范围内。

**4.2.5** 如果确定用 SIS，先定义目标安全完整性级别（SIL）（参见附录 A），建立 SIS 要求。SIL 定义为达到用户的过程安全目标所需的性能级别。SIL 定义为三个级别，3 级以上的级别不在本标准讨论范围内。SIL 级别越高，SIS 的安全性越高。增加冗余、增加实验次数、采用诊断故障检测、采用不同传感器及终端控制元件可以改进 SIS 性能。通过更好地控制设计、操作及维护程序也可以改进 SIS 性能。

SIL 与平均故障率有关（见表 4.1）。

**表 4.1 安全完整性级别性能要求**

完全完整性级别	1	2	3
SIS 性能要求	安全可靠性范围		
	0.9~0.99	0.99~0.999	0.999~0.9999
	平均故障率范围		
	$10^{-1} \sim 10^{-2}$	$10^{-2} \sim 10^{-3}$	$10^{-3} \sim 10^{-4}$

SIL 的概念用在安全生命周期的几个步骤中。参见附录 A 确定 SIL。完成此步骤的方法不在本标准范围内。

**4.2.6** 编制安全要求规格书。安全要求规格书列出了 SIS 功能和完整性要求（见第 5 章）。

**4.2.7** 进行 SIS 概念设计，满足安全要求规格书的要求（SRS）。附录 B 提供选择满足 SIL 要求的结构选择指导（见第 6 章）

**4.2.8** 完成 SIS 概念设计后，进行详细设计（见第 7 章）。

**4.2.9** 安装 SIS（见第 8 章）。

**4.2.10** 安装完毕后，应进行 SIS 调试和预启动认可试验（PSAT）（见第 8 章）。

**4.2.11** 在安全生命周期的任意一步都可以编制操作程序和维修程序，但应在启动前完成（见第 9 章）。

**4.2.12** 在启动 SIS 前，应进行预启动安全检查（PSSR）。PSSR 应包括下列 SIS 的活动：

- 确认 SIS 的建造、安装、试验符合安全要求规格书的要求；
- 与 SIS 有关的安全、操作、维修、变更管理（MOC）、应急步骤在适当的位置且足够；
- 用于 SIS 的 PHA 的建议已被采纳和处理；
- 包括 SIS 内容在内的员工培训已完成。

这些活动的计划和执行不在本标准的范围内。

**4.2.13** 完成 PSSR 后，SIS 可以运转。此步骤包括启动、正常操作、维修、周期性的功能试验（见第 9 章）。

**4.2.14** 如果提出修改，应按照变更管理（MOC）程序进行。安全生命周期中的有关步骤应重复，以反映变更对安全的影响（见第 10 章）。

**4.2.15** 有些时候，需要停运 SIS。例如，由于工厂关闭、拆迁或变更生产流程而停止 SIS。应有计划停运 SIS，宜采取适当的步骤保证以降低安全性的方式实现停运（见第 11 章）。

## 5 编制安全要求规格书

注：本章是本标准的主体部分，是强制性的要求。



## 5.1 目的

本章的目的是编制安全仪表系统（SIS）设计的规格书。安全要求规格书由安全功能性要求和安全完整性要求组成。安全要求规格书可以是一套文件或资料。

## 5.2 输入要求

编制安全要求规格书需要从过程危险分析（PHA）或过程设计组得到如下资料：

- 5.2.1 所需的安全功能清单和每个安全功能的安全完整性级别（SIL）。
- 5.2.2 每个需要 SIS 的潜在的危險事件的过程资料（偶然的原因、动态、终端元件等）。
- 5.2.3 过程公共原因故障需要考虑的事项，如腐蚀、堵塞、涂层破损等。
- 5.2.4 影响 SIS 的规则要求。

## 5.3 安全功能要求

安全功能要求应包括下列内容。

- 5.3.1 对每一个已确定的事件，定义其过程安全状态。
- 5.3.2 SIS 的过程输入及其跳闸设定值。
- 5.3.3 过程变量的正常操作范围及操作界限。
- 5.3.4 SIS 的过程输出及其作用。
- 5.3.5 过程输入输出的功能关系，包括逻辑、数学功能及所需的许可。
- 5.3.6 选择失电跳闸或得电跳闸。
- 5.3.7 考虑手动关断。
- 5.3.8 SIS 失电采取的动作。
- 5.3.9 SIS 使过程回到安全状态响应时间要求。
- 5.3.10 对任何显性故障的响应动作。
- 5.3.11 人机界面要求。
- 5.3.12 复位功能。

## 5.4 安全完整性要求

安全完整性要求应包括下列内容。

- 5.4.1 每个安全功能所需的 SIL。
- 5.4.2 达到所需的 SIL 的诊断要求（参见 B.9）。
- 5.4.3 达到所需的 SIL 的维修和试验要求。
- 5.4.4 如果谬误跳闸是危险的，对可靠性的要求。

## 6 SIS 概念设计

注：本章是本标准的主体部分，是强制性的要求。

### 6.1 目的

本章的目的是定义一些要求，这些要求用来开展和验证一个 SIS 概念设计满足安全要求规格书。

### 6.2 概念设计要求

- 6.2.1 每个安全功能所用的安全仪表系统（SIS）的结构选择应满足其所需的安全完整性级别（SIL）（如所选的结构是 1 选 1 [1001]、2 选 1 表决 [1002]、3 选 2 表决 [2003] 等）。
- 6.2.2 SIS 可以是具有单一的安全功能或具有一个公共逻辑控制器和（或）多个输入输出设备的多个安全功能。当多个安全功能共享公共元件时，公共元件应满足共享安全功能的最高 SIL。不是共享的系统元件必须满足各自所需的 SIL 要求。当多个 SIS 组合成一个系统并共享逻辑或元件时，公共原因潜在的故障会增加。需考虑的典型公共原因故障有编程、可达性、维护、电源及安全性。
- 6.2.3 应通过下列设计考虑的组合来满足所要求的 SIL：
  - a) 分离——同样的或者不同的（参见 B.1）；

- b) 冗余——同样的或者不同的 (参见 B.2);
- c) 软件设计考虑 (参见 B.3);
- d) 技术选择 (参见 B.4);
- e) 故障率和故障模式 (参见 B.5);
- f) 结构 (参见 B.6);
- g) 电源 (参见 B.7);
- h) 公共原因故障 (参见 B.8);
- i) 诊断 (参见 B.9);
- j) 现场设备 (参见 B.10);
- k) 用户界面 (参见 B.11);
- l) 安全性 (参见 B.12);
- m) 接线 (参见 B.13);
- n) 文件 (参见 B.14);
- o) 功能试验间隔 (参见 B.15)。

## 7 SIS 详细设计

注：本章是本标准的主体部分，是强制性的要求。

### 7.1 目的

本章的目的是提供安全仪表系统 (SIS) 设计的详细要求，达到安全要求规格书和概念设计的要求。

### 7.2 一般要求

7.2.1 SIS 设计应能够满足安全完整性级别 (SIL)。

7.2.2 SIS 可以包括顺序功能，使过程进入或维持在安全状态。

7.2.3 SIS 可以包括一个或多个联锁或安全功能。

7.2.4 SIS 设计文件的正式版本和发行控制程序应受控。

7.2.5 SIS 应用的设备制造厂商应保持正式版本和发行设备的控制程序，包括应用软件。可以使用标识或用户界面识别此信息 (例如，部分 #、系列 #、批量 # 等)。

7.2.6 设计应保证使用的硬件和软件是兼容的。

7.2.7 由 SIS 实现的非安全功能的动作不能中断或危及任何 SIS 的安全功能。

7.2.8 应定义安全功能需要的每个 SIS 的元件的安全状态。

7.2.9 SIS 应设计成当过程处于安全状态时，一直保持在安全状态除非进行复位。手动或自动复位应满足安全要求规格书的要求。

7.2.10 除非在安全要求规格书中有要求，应有独立于逻辑控制器的手动方法来启动 SIS 的终端元件。

7.2.11 任何检测到的引起 SIS 故障的单个故障应产生自动、预定的、安全故障动作，和 (或) 如果采用适当的响应动作，可将过程处于安全状态。

7.2.12 设计应采用满足环境和危险区域划分的规范和标准 [例如，NFPA 70 全国电气规程 (美国)，条款 500] (参考 C.5)。

7.2.13 除非传感器或终端元件是 7.4.2.2 和 7.4.3.1 允许公用的，SIS 输入/输出供电电路应和用于其他目的的电路分开。

### 7.3 SIS 逻辑控制器

7.3.1 逻辑控制器厂商应提供完整的设计，包括应用场合、输入模块、输出模块、维护接口设备、通信和公用软件等。整个设计应文件化。

**7.3.2** 逻辑控制器厂商应提供平均无故障时间 (MTTF)、隐性故障模式清单及识别的隐性故障发生的频率。应提供上述方法和数据源。

**7.3.3** PES 逻辑控制器应有防止隐性故障的方法 [内部和 (或) 外部]。(如逻辑控制器性能与过程动作的比较, 内置软件或应用软件测试逻辑控制器性能。)

**7.3.4** 逻辑控制器应与基础过程控制系统 (BPCS) 分开 (参见 B.1), 除非某些场合 BPCS 和 SIS 功能由一个逻辑控制器实现 (如, 燃气透平)。在这些场合, BPCS/SIS 逻辑控制器应满足 SIL (参考 C.1)。

**7.3.5** 逻辑控制器应设计成当电力恢复时, 保证过程不会自动启动, 除非过程危险分析指出这是允许的。

## 7.4 现场设备

### 7.4.1 通用要求

**7.4.1.1** 离散输入/输出通电跳闸电路应采取方法来保证电路的完整性。(例如, 尾端电阻检测, 如用先导电流连续检测, 保证电路的连续性; 先导电流幅度不能太大, 以免影响正常的 I/O 操作。)

**7.4.1.2** 当使用远程输入/输出时, 远程输入/输出应和逻辑控制器一起进行评估 (参见 B.6)。

**7.4.1.3** 除下列情况外, 每个单独的现场设备应具有自己专门的与系统输入/输出的接线:

- a) 如果多个传感器检测相同过程参数 (例如, 马达过载), 则多个离散传感器可串接在单个输入回路;
- b) 如果每个终端控制元件 (FCE) 用于相同过程条件, 则多个 FCE 可串接在单个输出回路;
- c) 用户批准的系统, 如火气探测系统;
- d) 参见 ISA SP50 现场总线的 1.2.10。

**7.4.1.4** 应正确选择和安装现场设备, 减少从过程和环境条件引起的错误信息故障。应考虑包括腐蚀、管道中的材料冻结、固体悬浮物、聚合物、炼焦、温度和压力极值的条件。

### 7.4.2 传感器要求

**7.4.2.1** 智能传感器应进行写保护, 防止远程误改动, 除非安全评估允许使用读/写。

**7.4.2.2** 用于 SIS 的传感器应和用于基础过程控制系统 (BPCS) 的传感器分开。在传感器故障不影响 SIS 进入保护状态的前提下, 允许有两个例外:

- a) 如果使用冗余传感器, 只要 BPCS 的任何故障不影响传感器的操作或不影响 SIS 正确读取传感器的能力, 传感器可以同时连接到 BPCS 和 SIS (参见 B.1.5);
- b) 如果 PHA 决定除了 BPCS 和 SIS 外, 采用一个或多个保护层提供传感器冗余保护 (参见附录 A)。

**7.4.2.3** 厂商或用户应根据需要提供传感器诊断功能, 满足所需的 SIL (参见 B.9)。

### 7.4.3 终端控制元件要求

**7.4.3.1** 对于 SIL 3, BPCS 的调节阀不能作为惟一的终端元件。对于 SIL 1 和 SIL 2, 使用一个 BPCS 的调节阀作为惟一的终端元件应进行安全评估 (参见 B.1.6)。

#### 7.4.3.2 马达启动器

除非过程危险分析另外要求, 通常 BPCS 和 SIS 公用马达启动器 (参见 B10.4.3)。

## 7.5 接口

本节讨论所有 SIS 的人—机界面和通信接口, 包括但不限于下列内容:

- a) 操作员界面;
- b) 维护/工程师界面;
- c) 通信接口。

### 7.5.1 操作员界面要求

操作员界面指操作员与 SIS 交换信息的媒体 (如 CRT、指示灯、按钮、喇叭、报警等)。

**7.5.1.1** 操作员界面系统的设计应考虑失去 SIS 操作员界面以及产生的要求（由安全评估定义），设计应保证 SIS 操作员界面故障时，应有其他方法使操作员将过程回到安全状态，SIS 的自动功能不受影响。

**7.5.1.2** 维护 SIL 重要的 SIS 状态信息应作为操作员界面的一部分。信息可能包括如下：

- a) 过程正在进行的序列；
- b) SIS 保护作用已经发生的指示；
- c) 保护功能被旁路的指示；
- d) 自动动作，如表决和（或）故障处理已发生的指示；
- e) 传感器和终端控制元件的状态；
- f) 如果失去电源影响安全时失去电源的情况；
- g) 比较诊断结果；
- h) 支持 SIS 必要的环境调节设备故障。

**7.5.1.3** 不允许从 SIS 操作员界面更改 SIS 的应用软件。当 SIS 的维护/工程师界面用作 SIS 的操作员界面时，从此界面修改应用软件应进行安全评估和需要进入密码。可能有些与安全有关的信息需要从 BPCS 传到 SIS。例如，在批处理系统中，SIS 根据所用的菜单可能有不同的设定或逻辑功能，这样，可以用操作员界面来选择 SIS 中的逻辑功能或选择菜单特用表格。对于此类应用，只能使用 SIS 系统，能够有选择地允许写入 SIS 的变量（该变量 BPCS 也可以进入），具有确认程序保证写入的选择已传到 SIS，SIS 已接收到（参见 B.1.8）。

只能使用维护/工程师界面，通过组态或编程过程，应用适当的文件和安全措施来实现允许或不允许读—写进入。操作员界面不能用于完成此功能。

#### **7.5.2 维护/工程师界面要求**

维护/工程师界面是用来维护 SIS 的媒体，包括可能在软件、编程终端、诊断工具、指示、旁路设备、试验设备和校验设备中发现的指令和诊断。

**7.5.2.1** 维护/工程师界面的设计，应保证该界面的任何故障不会反过来影响 SIS 将过程带回安全状态的能力。SIS 正常运行时，可能需要将维护/工程师界面（如编程盘）断开。

**7.5.2.2** 维护/工程师界面应提供下列功能：

- a) 进入 SIS 运行模式、程序、数据、失效报警通信的工具、试验、旁路、维护等需有密码保护；
- b) 可以进入 SIS 诊断、表决和故障处理服务；
- c) 可以增加、删除或修改应用软件；
- d) 可以进入处理 SIS 故障必需的数据。

#### **7.5.3 通信接口要求**

通信接口指 SIS 和其他设备（如操作员界面、维护/工程师界面、BPCS、网络或外围设备）之间的硬件和软件通信。

**7.5.3.1** 通信接口的设计应保证接口的任何故障不会反过来影响 SIS 将过程带回安全状态的能力。

**7.5.3.2** 通信信号应通过采用好的工程方法与其他能源隔离。例如，单一专用电源使用屏蔽电缆并保持单独接地，或使用光缆。

#### **7.6 电源**

设计应保证每个电源满足安全要求规格书中规定的 SIS 的要求（参见 B.7）。

#### **7.7 系统环境**

系统环境必须保证 SIS 的正常运行。系统环境可能需要考虑的因素：温度、湿度、污染物、接地、电磁干扰/射频干扰（EMI/RFI）、振动、静电释放、电气区域划分和溢流水淹等。

**7.7.1** 在系统设计中应考虑 SIS 所处的环境条件及 SIS 所有元件对操作环境的要求。

**7.7.2** 系统设计应采取特殊步骤解决环境条件与设备要求之间的差异，如安装加热、通风/空调设

备、和（或）空气过滤器，使得 SIS 满足安全要求规格书。

## 7.8 应用逻辑要求

### 7.8.1 电气系统应用逻辑

7.8.1.1 应提供惟一的受控正式修订版应用逻辑和发行控制程序用于 SIS。

7.8.1.2 应提供应用逻辑正式修订版和发行控制程序，并由用户维护。

7.8.1.3 用户应保证应用逻辑存档清楚、明确、完整（参考 B.14）。

### 7.8.2 电子系统应用逻辑

7.8.2.1 应提供惟一的受控正式修订版应用逻辑和发行控制程序用于 SIS。

7.8.2.2 应提供应用逻辑正式修订版和发行控制程序，并由用户维护。

7.8.2.3 用户应保证应用逻辑存档清楚、明确、完整（参见 B.14）。

### 7.8.3 可编程电子系统应用逻辑

本节讨论的软件介绍 SIS 的应用。如果内置软件和公用软件影响应用软件也将进行讨论。

7.8.3.1 应提供惟一的受控正式修订版应用逻辑和发行控制程序，用于 SIS。

7.8.3.2 应提供内置软件和公用软件受控正式修订版和发行控制程序，并由 SIS 制造商维护。制造商也应提供和保留故障清单，并告知用户任何可能导致功能请求失败的软件故障。

7.8.3.3 用户不能修改 SIS 的内置软件和公用软件。

7.8.3.4 用户应保证应用软件存档清楚、明确、完整（参见 B.3 和 B.14）。

7.8.3.5 应用软件正式修订版和发行控制程序应由用户维护。

## 7.9 维护或测试设计要求

7.9.1 设计应允许测试整个系统。应能够测试终端元件响应传感器作用的动作。当计划的过程停工期间间隔大于功能试验间隔时，则需要在线测试设备。

7.9.2 当需要在线功能试验时，测试设备应是 SIS 设计的一部分，能够测试隐性故障。

7.9.3 当测试和（或）旁路设备包括在 SIS 中时，应满足下列要求：

- a) SIS 须根据安全要求规格书中定义的维护和测试要求进行设计；
- b) SIS 任何部分的旁路应通过报警和（或）操作步骤警告操作者；
- c) SIS 任何部分的旁路不能导致失去检测和（或）正检测的报警。

7.9.4 强制输入和输出不能用在下列的部分：

- a) 应用软件；
- b) 操作步骤；
- c) 除注明外的维护。

SIS 运行时，除非程序补充和执行加密，不允许强制输入和输出。强制输入和输出时应有报警。

## 8 安装、调试和预启动认可试验

注：本章是本标准的主体部分，是强制性的要求。

### 8.1 目的

8.1.1 本章的目的是保证安全仪表系统根据详细设计进行安装，并且性能符合安全要求规格书。

8.1.2 安装、调试或预启动认可试验（PSAT）时，SIS 设备的任何修改或变更应回到安全生命周期的有关阶段（最初的变更影响）。

### 8.2 安装

8.2.1 任何设备应根据设计要求安装。

### 8.3 调试

8.3.1 调试保证 SIS 是根据详细设计要求安装，可以进行预启动认可试验。

8.3.2 SIS 调试工作包括检查（但不限于检查）下列内容是根据详细设计文件安装的，性能符合安

全要求规格书的要求。

- a) 设备和接线安装正确；
- b) 动力源正常；
- c) 所有仪表已经过校验；
- d) 现场设备正常；
- e) 逻辑控制器和输入/输出正常。

#### 8.4 预启动认可试验 (PSAT)

8.4.1 预启动认可试验提供 SIS 全功能试验，证明符合安全要求规格书。预启动认可试验应包括但不限于确认下列内容：

- a) SIS 与基础过程控制系统或其他系统或网络通信正常（如要求）；
- b) 传感器、逻辑、计算及终端控制元件性能符合安全要求规格书；
- c) 安全设备在安全要求规格书中定义的设定点处动作；
- d) 关断顺序动作正确；
- e) SIS 提供正确的报警和操作显示；
- f) SIS 中包括的计算精度；
- g) 根据计划，系统全部复位和部分复位功能；
- h) 旁路和旁路复位动作正确；
- i) 手动关断系统动作正确；
- j) 试验间隔时间在维护程序中有说明，符合 SIL 要求；
- k) SIS 文件符合实际安装和操作系统。

8.4.2 在 SIS 设计所避免或减缓的危险进入之前，应完成预启动认可试验。

8.4.3 在 PSAT 中所用测试仪表的校验精度应与应用要求相符。例如 SIS 设定点与危险过程情形之间的裕度可以用来确定所需的精度。

8.4.4 在 SIS 设计预防和减缓的危险进入之前，证明调试和 PSAT 已完成的文件应完成。证明文件至少应包括下列内容：

- a) SIS 已试验的标识；
- b) 调试已完成的证明；
- c) PSAT 完成的日期；
- d) 用于 PSAT 中的参考文件；
- e) 表明 PSAT 已圆满完成的权威签署。

### 9 SIS 操作和维护

注：本章是本标准的主体部分，是强制性的要求。

#### 9.1 目的

本章的目的是保证安全仪表系统功能在整个运行过程中符合安全要求规格书。

#### 9.2 培训

9.2.1 从事 SIS 操作和维护工作的雇员应经过有关培训。

9.2.2 雇员培训应遵守所用规章的要求（如 OSHA 29 CFR1910.119，参考 C.11）。

#### 9.3 文件

用户应具有相关的文件（如第 9 章各节所要求），应使用最新版文件（参见 B.14）。

#### 9.4 SIS 操作程序

应编制阐述 SIS 安全正确操作方法的操作程序，这些程序通常是单元操作程序的典型部分。操作程序应包括但不限于下列内容：

- a) 安全操作的界限（如关断点）和超限的安全含义；
- b) SIS 如何将过程回到安全状态；
- c) 正确使用旁路、许可、系统复位等（需要时）；
- d) SIS 报警和关断的正确响应。

## 9.5 维护程序

9.5.1 应编制维护程序。维护程序应包括维护、试验和维修 SIS 的书面程序。

9.5.2 SIS 维护程序应包括，但不限于下列内容：

- a) SIS 定期功能测试；
- b) 如需要，定期预防维护（如替换通风滤网、润滑油、电池更换、校验等）；
- c) 修复检测到的故障，修复后进行试验。

## 9.6 测试、检验和维护

9.6.1 描述 SIS 维护和测试要求（如电池维护、保险丝更换）的厂商手册可以包括在维护程序中。

9.6.2 旁路可能是必要的。如 SIS 功能被旁路，而过程是危险的，应提供行政管理控制和书面的程序来维护过程的安全性。

9.6.3 用户应有 SIS 检测设备故障、缺陷等周期性的检查程序。

## 9.7 功能试验

并非所有系统故障是自己暴露的。那种可能抑制 SIS 在需要时动作的隐性故障只有在试验整个系统时才能检测到。

9.7.1 周期性功能试验应按编制的程序进行（见 9.7.4.1），根据安全要求规格书检测阻止 SIS 操作的隐性故障。

9.7.2 应测试整个 SIS，包括传感器、逻辑控制器和终端元件（如关断阀、马达）。

9.7.3 功能测试频率：

9.7.3.1 SIS 应根据安全要求规格书中规定的频率定期进行测试（参见 B.15）。注意 SIS 不同部分可能需要不同的测试时间间隔。

9.7.3.2 在某些周期间隔（由用户确定），对 SIS 或 SIS 中的部分测试的频率应根据历史数据、工厂经验、硬件老化、软件可靠性等重新评估。

9.7.3.3 应用逻辑的任何变更都需要完整的功能试验，除非已进行过检查和部分试验保证 SIL 没有降低。

9.7.4 功能测试程序：

9.7.4.1 对每个 SIS，应提供描述所要进行的每一步骤的文件化功能测试程序。

9.7.4.2 功能测试中发现的任何缺陷应安全及时地修正。

9.7.4.3 功能测试程序应包括，但不限于验证下列内容：

- a) 运行所有输入设备，包括一次传感器和 SIS 输入模块；
- b) 与每个输入设备有关的逻辑；
- c) 与组合输入有关的逻辑；
- d) 所有输入的关断点（设定点）；
- e) 报警功能；
- f) 需要时，SIS 的响应速度；
- g) 逻辑程序的运行顺序；
- h) 所有终端控制设备的功能和 SIS 输出模块；
- i) SIS 完成的计算功能；
- j) 使系统回到安全状态的手动关断功能；
- k) 用户诊断功能；

- l) 完成系统功能;
- m) 测试完成后, SIS 正常。

#### 9.7.5 在线功能测试:

##### 9.7.5.1 应编写(如需要)允许在线功能测试的程序。

##### 9.7.5.2 对实际不能进行关断测试的终端元件,应编写包括如下内容的程序:

- a) 在单元关断时测试终端元件;
- b) 在线测试时尽可能试验输出(如输出跳闸继电器、关断电磁阀、阀门部分动作)。

#### 9.8 功能测试文件编制

##### 9.8.1 应编制进行的所有测试说明。用户应保留证明测试和检查已完成的记录。

##### 9.8.2 文件编制至少包括下列内容:

- a) 检查的日期;
- b) 进行测试或检查的人员姓名;
- c) 设备的系列号或其他标识(回路号、编号、设备号、用户认可的号等);
- d) 检查/测试结果(“发现的”和“遗留的”情况)。

### 10 SIS 变更管理(MOC)

注:本章是本标准的主体部分,是强制性的要求。

#### 10.1 目的

本章的目的是保证变更管理要求应用于运行中的 SIS 的任何变更中。

#### 10.2 变更管理(MOC)程序

##### 10.2.1 书面程序应放置在适当的位置,用以启动、记录、检查和批准 SIS 的变更,而不是“同类替代”(如 OSHA 29 CFR 1910.119, Section “B”)(参考 C.11)。

下列情况可能需要 MOC 程序:

- a) 更改操作步骤;
- b) 由于新的或修订后的安全立法要求所需的更改;
- c) 更改工艺流程;
- d) 更改安全要求规格书;
- e) 更改软件或固体的错误;
- f) 修改更正系统故障;
- g) 由于故障率高于期望值的更改;
- h) 由于 SIS 期望值增加的更改;
- i) 更改软件(内置、公用和应用软件)。

##### 10.2.2 MOC 程序应保证在进行变更前考虑下列问题:

- a) 所要变更的技术基础;
- b) 变更对安全和健康的影响;
- c) 操作步骤的修改;
- d) 变更所需的时间;
- e) 权威部门对变更的要求;
- f) 内存空间的可用性;
- g) 对响应时间的影响;
- h) 在线对离线的变更和包括的风险。

##### 10.2.3 变更的检查应保证:

- a) 维持所要求的安全完整性;



b) 有关专业的人员参加检查过程。

10.2.4 在完成变更或启动过程时, 应事先告知变更所影响的人员相应的变更并对其进行培训。

10.2.5 SIS 的所有变更应返回至安全生命周期的适当阶段 (变更所影响的第一阶段)。并执行安全生命周期的随后所有阶段, 包括验证变更已正确执行且已编制成文。所有变更的执行 (包括应用软件) 应遵守前面建立的 SIS 设计步骤。

### 10.3 变更管理文件

10.3.1 在启动和更新前, 应记录操作程序的所有变更、过程安全资料和 SIS 文件 (包括软件)。

10.3.2 应保护文件以防未经授权的修改、损坏或丢失。

10.3.3 所有 SIS 文件应修改、修正、检查、批准, 应按适当的文件控制程序来管理。

## 11 停运

注: 本章是本标准的主体部分, 是强制性的要求。

### 11.1 目的

11.1.1 保证在安全仪表系统 (SIS) 永久停止运行前进行检查。

### 11.2 通则

11.2.1 所有停运活动应执行变更管理程序 (见第 10 章)。

11.2.2 停运前, 应评估停运 SIS 对相邻操作单元和设施的影响。

## 12 差异

注: 本章是本标准的主体部分。本章阐述 ISA-S84.01 和 IEC 草案出版物 1508 之间的主要不同点。

总的说来, ISA-S84.01 与 IEC 1995 年草案出版物 1508 第 1 部分~第 7 部分不同。这些不同点在 12.1, 12.2 和 12.3 中进行阐述, 是对 S84.01 与 1995 年草案出版物 1508 的比较。草案出版物 1508 将有大的变化。IEC 草案出版物 1508 正式出版时, 如需要, SP84 委员会将重新修改第 12 章, 重新出版 S84.01。

本章仅将 IEC 草案出版物 1508 标准部分 (即第 1 部分、第 2 部分、第 3 部分、第 4 部分) 与 ISA-S84.01 进行比较。

安全仪表系统所用的操作模式分为如下模式:

a) 期望模式: SIS 的设计应具有一定的失效概率, 从而用来完成其要求达到的设计功能;

b) 连续模式: SIS 用来取得每年一定的危险故障率 (如航空电子学)。本标准不讨论操作连续模式。

### 12.1 术语差异

术语差异见表 12.1。

表 12.1 术语差异

IEC 草案出版物 1508 (第 4 部分)	ISA-S84.01	注 释
E/E/PES 安全有关的系统	SIS	IEC 草案出版物 1508 中描述的安全有关的系统采用所有技术, 而 S84.01 描述的技术仅指安全仪表系统

表 12.1 (续)

IEC 草案出版物 1508 (第 4 部分)	ISA-S84.01	注 释
PES	PES	IEC 草案出版物 1508 中“PES”包括传感器和终端控制元件, 而 S84.01 中的“PES”不包括传感器和终端控制元件
EUC	过程	IEC 草案出版物 1508 使用“EUC 受控设备”作为一般术语, S84.01 使用过程作为一般术语
评估	PSSR	IEC 草案出版物 1508 中使用评估, 而 S84.01 使用确认和预启动安全检查 (PSSR)
功能要求规格书	安全要求规格书	IEC 草案出版物 1508 中使用功能性要求规格书, S84.01 使用安全要求规格书

12.2 组织差异

ISA-S84.01 是由仪表人员为 ISA、测量与控制国际协会和美国国家标准化组织 (ANSI) 编制的。因此, 该标准没有详细的过程危险评估内容, 而目前美国规范如 OSHA 29 CFR 1910.119 对过程危险评估有强制要求。

S84.01 对培训、变更管理、人员证书、过程危险评估只做简单讨论, 提供参考, IEC 对这些问题的讨论更加深入。组织差异见表 12.2。

表 12.2 组织差异

IEC 草案出版物 1508 (第 1 部分)	ISA-S84.01
规定外部风险减少设施功能的安全的要求	没有外部风险减少设施功能的安全的要求
适用于所有安全相关系统和外部风险减少设施	只适用于 E/E/PES 安全相关的系统 (如 SIS)
将安全完整性级别用于外部风险减少设施	没有将安全完整性级别用于外部风险减少设施
强制使用 ISO 9000 系列质量体系或等效体系	没有强制使用 ISO 9000 系列质量体系或等效体系
强制使用 IEC 草案出版物 1508 中的表格“人员、部门、组织独立性最小级别”	没有强制使用 IEC 草案出版物 1508 中的表格
要求记录没有实现 IEC 草案出版物 1508 中“强烈推荐”措施或技术的理由	没有要求记录使用不同实现方案的原因
强制使用安全计划 (详见下列)	要求文件符合 OSHA 1910.119, 参考 C.11 - 对安全计划没有要求
(4.6) 强制坚持相关措施和技术	没有强制坚持任何特定措施和技术 要求使用好的工程惯例

表 12.2 (续)

IEC 草案出版物 1508 (第 1 部分)		ISA – S84.01
(4.6) 强制目击试验确保符合该标准		没有强制目击试验确保符合标准
(5) 除了 ISO 9000 外, 通过提供详细要求, 讨论“人员的能力”		参考 OSHA 1910.119 中“人员的能力”及参考 C.11
(6.0) 定义整个安全生命周期中“安全管理”活动		除变更管理外, 没有提到管理问题
(7.1) 强制整个安全生命周期每一阶段都有确认活动, 设计检查、试验和分析结果有文件记录		强制 SIS 的运转和预启动认可试验 (PSAT) 有适当的文件记录 (见 8.3 和 8.4)
(7.1.3.2) 强制安全生命周期所有方面使用 ISO 9000 程序和 IEC 1508 草案出版物		没有要求使用 ISO 9000
(7.1.3.1) 强制执行安全生命周期每一步骤, 提供定义偏差的书面安全计划		没有提到过程概念设计、过程危险和风险分析、非 SIS 保护层、需要 SIS 和决定所需的 SIL SP84 要求在执行 SP84 前完成这些活动
(7.1.3.3) 强制整个安全生命周期每一阶段分为基础任务, 具有定义好的输入/输出活动范围和文件记录		
(7.2) 需要过程概念设计资料和总体过程概念描述		实现的方法不在本标准的范围内
(7.3) 需要在总体范围定义描述中定义 EUC		
(7.4) 定义危险和风险分析, 要求有实现的方法和文件记录		
(7.5) 要求	条 目	实现的方法不在本标准的范围内
风险降低	7.5.2.4	
	7.5.2.6	
	7.5.2.7	
所有安全功能	7.5.2.2	
安全级别	7.5.2.3	
规定降低风险的方法	7.5.2.5	实现的方法不存在本标准的范围内
(7.6.1) 安全要求配置是由 PHA 决定, 有外部风险降低设施		
(7.7) (7.15) 全部操作员和维护计划, 包括外部危险降低系统分析		
(7.8) (7.14) 确认包括外部风险降低		
(7.9) (7.13) 提供安装要求		参考 OSHA 1910.119 中的变更管理, 参考 C.11
强制全面修改和更新		

表 12.2 (续)

IEC 草案出版物 1508 (第 1 部分)	ISA - S84.01
强制停运记录、确认计划、功能性安全评估计划和报告、独立性级别	没有规定这些要求
提到所有阶段文件	仅提到 SIS 文件
第 2 部分和第 3 部分是标准	第 2 部分和第 3 部分部分是标准，部分作为参考——待定

12.3 技术差异

技术差异见表 12.3。

表 12.3 技术差异

IEC 草案出版物 1508	ISA - S84.01	注 释
SIL 1, SIL 2, SIL 3, SIL 4	SIL 1, SIL 2, SIL 3	S84.01 没有提到安全完整性级别 (SIL) 4, 也不认可其存在, SIL 4 在工业生产过程中通常没有
EUC (受控设备) 控制系统不包括安全控制	基础过程控制系统 (BPCS)	IEC 草案出版物 1508 使用 EUC 控制系统, 而 S84.01 使用 BPCS

## 附 录 A (资料性附录)

### 决定安全仪表系统 (SIS) 安全完整性级别 (SIL) 示例

注：本附录不是本标准的强制要求，仅供参考。

#### A.1 简介

本附录提供了 4 个有关确定安全完整性级别 (SIL) 的方法的案例，确定安全完整性级别是过程安全活动的一部分。这些案例仅提供了有关确定 SIL 方法的范围与类型的一般性资料。附录 C 中所指出的 [参考 C.1] 描述了这些方法及其他方法。对于确定在什么地方采用什么仪表安全系统合适、什么过程变量启动仪表安全系统以及最终在过程上采取什么措施则不包括在本附录的范围内。通过将这 4 种确定 SIL 的方法用到一个实例中，仅够详细地概念性地表明了如何确定安全完整性级别 (SIL)。参考书目详细描述了如何理解和使用这些确定安全完整性级别的方法。

选取了 4 种 SIL 的决定方法来举例说明各种处理方法。选择一种简单的矩阵法来简单表明关键因素，由此可以认识到其他可用的较复杂的矩阵方法。只看后果法举例说明了一种直接的安全完整性级别 (SIL) 的选择方法，该方法采用了一些很保守的安全前提。为定性评估 SIL 确定方法的风险，选用了一种改进的 HAZOP 法。通过描述如何采用故障树分析来确立 SIL，描述了风险的定性评估方法。

无论运用何种方法来确定 SIL，都是作为过程安全活动的一部分。决定 SIL 是过程安全小组的一项职责，过程安全小组包含有各种相关的专门技术的参与者。一般来说，过程安全小组中包含有如下专门知识和资格的人员是合适的：

- a) 业主——直接负责设备操作的人员；
- b) 过程知识——了解过程及设备操作的基本科学技术；
- c) 设计知识——关于设备或者过程系统应该如何工作方面的知识，特别是有关复杂控制系统中的仪表的知识；
- d) 操作经验——那些具有直接操作及维修经验的人；
- e) 其他——进行过程危险审查的技能和所需的其他适当知识。

本附录没有提供足够的资料以充分了解任何方法，没有明示或暗示任何安全准则，也没有推荐任何专门方法。

如本标准第 4 章所描述，决定安全仪表系统 (SIS) 的安全完整性级别 (SIL) 是过程安全活动的一部分。如安全生命周期所描述，(见图 4.1)，步骤 2、步骤 3、步骤 4、步骤 5 和步骤 6 总结了包含在确定 SIL 中的过程安全概念。这些步骤如下：

- 步骤 2——评估危险事件的后果及发生的可能性；
- 步骤 3——除 SIS 之外，评估危险事件的预防、保护和对过程安全性能的减弱；
- 步骤 4——决定仪表安全系统 (SIS) 对某场合是否合适；
- 步骤 5——确定仪表安全系统的目标级别 (SIL)；
- 步骤 6——确定其他有关过程安全的技术规格书及设计准则。

过程安全活动的目标是有助于确保过程系统的安全操作，过程安全活动包括后果分析和过程危险审查 (参考 C.14 和参考 C.15)。对危险及危险事件进行识别，并确定控制风险及潜在隐患的方法是安全活动的一部分。控制风险和降低风险是根据过程的许多过程安全特性决定的，包括多项内容，如程序、基础过程设计、过压保护和 SIS。

#### A.2 安全完整性级别 (SIL) 的考虑方法和过程实例

安全完整性级别 (SIL) 是本标准的一个基本的概念。SIL 定义了 SIS 安全性能级别。SIL 被定

义为 1 级、2 级或 3 级。SIL 的级数越高, 该安全仪表系统执行的安全性能越好。较好的安全性能是通过较高的安全功能的可用性来达到的。仪表安全性能通过增加冗余, 增加测试频率, 运用故障自诊断等手段来改善, 本标准及附录对这些手段进行了描述。

对安全完整性级别 (SIL) 的 3 个级别如何实现的了解对于过程安全小组决定 SIL 将是重要的。当小组成员学习过程和危险事件是如何发生时, 他们就会知道仪表安全系统是如何执行安全功能的。了解了安全仪表系统 (SIS) 包括在什么样的场合该达到什么样的安全完整性级别 (SIL) 的重要性, 该小组就会有助于确保过程的设计和不会降低 SIS 的性能。

图 A.1 概念性地表示了 3 个安全完整性级别在该事例给出的场合中是如何实现的。图 A.1 描述的执行过程是本例特用的。如本标准及 ISA-dTR84.02 (参考 C.2) 所述, 有许多方法来构成安全仪表系统以达到特定的安全完整性级别。

图 A.2 描述了一个简单的管线仪表图 (P&ID), 作为工艺过程示例。高压蒸气用来控制低压系统的压力。低压系统通过以下措施进行过压保护:

- a) 泄压阀;
- b) 压力控制系统;
- c) 操作者对高压报警的处理。

通过关闭从高压系统到低压系统的物流, 或者打开低压系统的泄压阀来达到保护低压系统的目的。低压系统过压的后果是低压容器的爆裂。

过程安全小组确定了一个可能的安全仪表系统来防止低压系统的过压。安全仪表系统通过检测压力和关闭阀门来实现, 不同的安全完整性级别 (SIL) 有不同的阀门配置, 如图 A.1 所示该安全仪表系统由传感器、最终执行元件和逻辑控制器组成。图 A.2 简单表示了该工艺过程, 没有描述任何特定的 SIL 的要求。

### A.3 选择安全完整性级别 (SIL) 的方法示例

以下部分描述选择 SIL 用于该高压系统关断 SIS 的 4 种不同方法。

#### A.3.1 方法示例——安全保护层矩阵 (参考 C.1)

该方法基于对过程危险的定性理解, 需要对对于安全仪表系统和其他保护措施在整个事件发生过程中不起作用而产生潜在后果的危害及影响有一个定性的评估。需要识别所有各种发生的事件及其潜在的后果。

该方法使用定性矩阵, 如图 A.3, 需要一个对所有会导致不良后果的事件及除仪表安全系统 (SIS) 外的保护措施的有效性进行的评估。对决定矩阵输入值从低到高的范围的定性指南随诸如公司指南、地方的因素、工艺过程的性质等不同而不同。本例中的矩阵完全用于例证的目的。矩阵的应用实际上通常是依赖于公司的情况。

矩阵的应用需要对危险事件后果的严重程度进行定性的评估, 这些危险事件正是仪表安全系统 (SIS) 要防止的。该实例中过程安全小组认为严重程度适中。

矩阵的应用也需要对会导致不良后果的事件发生的可能性进行定性的评估。该实例中过程安全小组认为会导致不良后果的事件发生的可能性适中。

矩阵的第三个轴要求对其他保护层次的有效性做出定性评估。除考虑 SIS 外, 要评估其他保护层在防止发生的事件导致后果的有效性。该实例中过程安全小组认为其有效性居于中低之间。该判断是基于需要操作者做出极快速的反应和泄压阀会堵塞做出的。通过这些定性的评估, 该矩阵指示该高压关断系统的安全级别是 2 级 (SIL 2)。

#### A.3.2 方法示例——只看后果的方法

该方法比起其他方法步骤较少, 只需要对当安全仪表系统及其他保护措施失效时可能产生后果的严重性进行评估。由于该方法减少了花在评估上的时间, 加快了安全完整性级别 (SIL) 的决定, 过

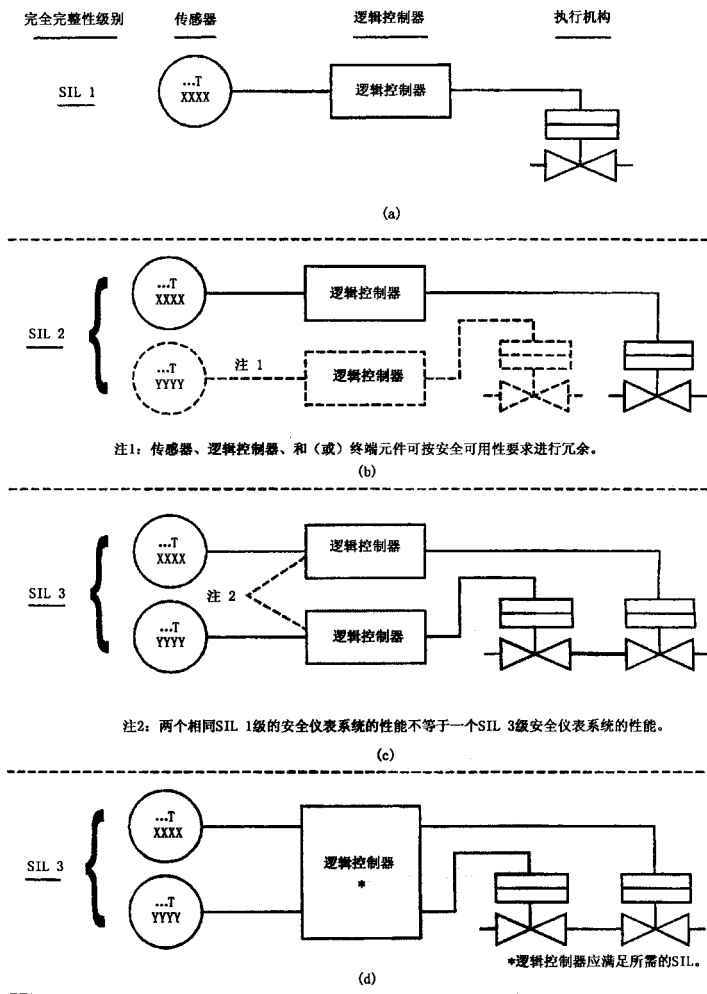


图 A.1 ABC 公司 × × 现场特定的 SIL 实现技术, 只作为示例

程安全小组认为该方法适用。不足之处是选出的安全级别(SIL)可能比其他方法选出的要高。过程安全小组会感觉按高于实际要求的安全级别进行设计是保守的。过程安全小组更喜欢节省用于风险评估的时间而承担由于选择较高的安全级别带来的费用。在安全性能与实际要求相同或更好的仪表安全系统上花费费用可以说是物有所值的。

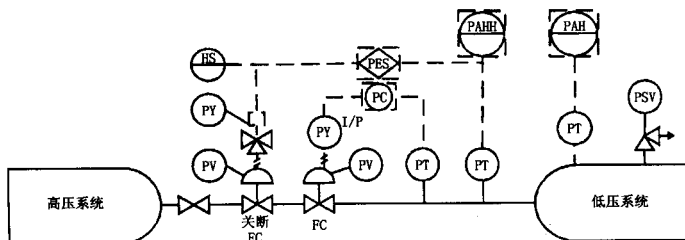


图 A.2 工艺过程示例

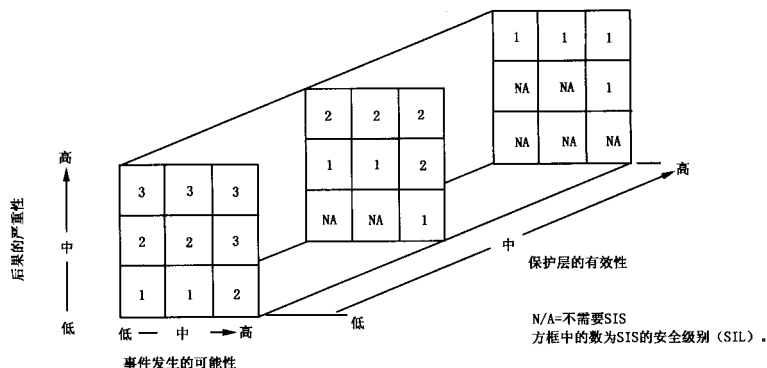


图 A.3 ABC 公司 × × 现场决定安全完整性级别 (SIL) 的定性矩阵示例

该方法只需要评估仪表安全系统及其他安全措施失效所带来的后果的严重性。因该方法保守，该装置将 SIL 从 3 个级别简化为 2 个级别，即在设计中只选择 SIL 1 级或者 SIL 3 级。如果后果的严重性高于基本阈值，则选 SIL 1 级。如果后果的严重性高于“主要”严重性参数，则选 SIL 3 级。

这两级严重性级别的定义包括人身伤害、财产损失和环境对工艺过程的影响。通过设想配有安全仪表系统的场合发生故障的频率是经常还是“可能”，从而在设定这些指南中表明有风险。

该实例中，过程安全小组评估了高压关断系统故障后果的严重性，觉得超过了“主要”参数。基于这些评估，选择了 SIL 3 级。

### A.3.3 方法示例——改进的 HAZOP 法

为确定安全级别，改进的 HAZOP 法包括了对后果的严重性、发生的可能性以及其他相关风险因素的考虑。从减低风险的有效性方面评估专门的减低风险的建议。基于这些评估过程，过程安全小组决定是否采用这些推荐意见，或者决定现在的风险控制措施是否足够。

使用一个在 HAZOP 分析法上富有经验的负责人，运用一套指南对过程流程分段地系统地进行分析以识别出可能导致危险事件的过程上的偏差。数据表格可用来将过程偏差与特定的干扰原因联系起来分析。随着这些干扰原因而来的是潜在的由干扰引起的后果、防止或阻止后果发生的因素以及安全小组对如何控制风险的判断和措施。基于这些评估过程，过程安全小组决定这些推荐意见，或者决定现在的风险控制措施是否足够。

用于该实例的部分改进的 HAZOP 法的文件列于表 A.1。



使用改进的 HAZOP 法的过程安全小组也识别出在启动阶段手动模式下操作者的错误，这个错误是产生高压干扰的一个原因。

基于后果的严重性、对于扰因素产生可能性的感觉和保护系统的整体性能，安全小组同意需要一个安全仪表系统。起初，过程安全小组考虑了 2 级或 3 级以待进一步评估。在考虑了安全、设备可靠性、以及操作维修费用后，小组决定 SIL 2 级安全仪表系统对该场合是更合适的。

表 A.1 改进的 HAZOP 文件示例

过程偏差	原因	后果	保护
流量超过正常值	压力调节阀故障打开	压力容器爆裂，从而产生潜在的人身伤害、财产损失和环境破坏	泄压阀； 操作者迅速对高压报警做出响应； 高压关断安全仪表系统
超压	压力传感器故障，产生漂移，压力输出值偏低		除操作者的响应只由一个高压信号引起外，其余与上述同

#### A.3.4 方法示例——从故障树决定 SIL

基于示例中容器爆裂危险和其他几种主要处理过程中的危险，对该例中的大部分过程做了故障树分析。该故障树定量分析了几种过程处理容器产生过压爆裂的频率。

故障树是一种系统表示故障后果的逻辑图表。从诸如传感器故障等基本事件开始一直到所谓的“顶级”事件，均一一列于图表中。该案例中的顶级事件是处理容器的过压爆裂。

通过对故障树逻辑图的分析能估算出顶级事件发生的频率。每个基本事件都被赋予了故障率和条件故障的可能性，然后就能估算出顶级事件发生的频率。[参考 C.1] 简单描述了故障树的分析方法，[参考 C.13] 全面地阐述了该分析方法。该实例的故障树细节过于复杂，因而本附录不进行描述。

在本案例中，使用故障树来确定 SIL 的第一步是画出故障树逻辑图。最初的故障树基于假定的图 A.2 所示的高压关断系统即 1 级安全级别。要决定与本案例有关的所有的事件的合适的故障信息。例如，像压力调节阀故障打开等事件发生的频率，然后就能计算出容器爆裂事故发生的频率。

在审查了该故障树的结果后，小组决定进行级别为 SIL 2 级和 SIL 3 级评估。随后的故障树的评估结果指出 SIL 2 级设计相对于 SIL 1 级设计安全性提高很多。容器爆裂的顶级事件的发生率降低了很大的百分数。对 SIL 2 级和 SIL 3 级做相同的比较后发现在安全上只有小的改进即顶级事件的发生率只有少许的减少。基于这些比较，小组将该高压关断系统定为 SIL 2 级。

**附 录 B**  
**(资料性附录)**

**SIS 设计需要考虑的问题**

注：本附录不是本标准的强制要求，仅供参考。

本附录论述满足 SIL 要求的各种设计方法，下面是 SIS 设计需要考虑的问题：

- B.1 分离——同样的或者不同的
- B.2 冗余——同样的或者不同的
- B.3 软件设计考虑
- B.4 技术选择
- B.5 故障率和故障模式
- B.6 结构
- B.7 动力源
- B.8 公共原因故障
- B.9 诊断
- B.10 现场设备
- B.11 用户界面
- B.12 安全
- B.13 接线
- B.14 文件
- B.15 功能测试时间间隔

**B.1 分离——同样的或者不同的**

**B.1.1** 分离 BPCS 和 SIS 的功能减少了控制和安全功能同时失效的可能性，或者减少了无意中的改变影响 SIS 安全作用的可能性。因此，一般来说 BPCS 和 SIS 的功能需要分离。

**B.1.2** 同样的分离通常在 SIL 1 级应用的场合可以接受。不同的分离另外具有减少系统性故障（在 SIL 3 级应用的场合这是一个特别重要的因素）的可能性和减少公共原因故障的优点（参见 B.8）。

**B.1.3** 可能需要 4 个方面的分离来满足安全的功能性和安全的完整性要求：

- a) 现场检测元件的应用；
- b) 终端控制单元的应用；
- c) 逻辑控制单元；
- d) SIS 与 BPCS 或其他设备之间的通信。

**B.1.4** 这 4 个方面中的每一个都应该进行评估以保证 SIL 的要求能够被满足。

**B.1.5** 检测元件：单个检测元件同时用在 BPCS 和 SIS 系统中，作为过程安全活动（附录 A）的一部分，需要做进一步的安全审查和安全分析。例如，一个液位检测元件既用做 BPCS 的液位控制又用做 SIS 的高液位关断，如果该检测元件在低于液位控制器设定点的位置出现了故障，液位控制器可能指挥进料阀门打开而这时高液位关断保护已失效。

**B.1.5.1** 对于 SIL 1 级，只要满足安全完整性的要求，单个检测元件可以同时用在 BPCS 和 SIS 系统。

**B.1.5.2** 对于 SIL 2 级，为了满足安全完整性的要求，BPCS 和 SIS 系统同样分离是通常需要。

**B.1.5.3** 对于 SIL 3 级，为了满足安全完整性的要求，BPCS 和 SIS 系统同样分离或者不同分离是通常需要。

**B.1.5.4** 当使用冗余的 SIS 检测元件时，这些检测元件可以同时接到 BPCS 和 SIS 系统，只要安全审查和安全分析表明检测元件接到 BPCS 并不会危及 SIS 系统的安全完整性。

**B.1.6 控制和关断阀门：**

**B.1.6.1** 对于 SIL 1 级，只要阀门的不安全故障率满足安全完整性的要求，单个阀门可以同时用在 BPCS 和 SIS 系统，设计上应确保 SIS 的动作优先于 BPCS 的动作。

**B.1.6.2** 对于 SIL 2 级，为了满足安全完整性的要求，BPCS 和 SIS 系统同样分离是通常需要。单个阀门同时用在 BPCS 和 SIS 系统，由于它可能不满足安全完整性的要求需要做进一步的安全审查和安全分析。例如，一个阀门既用做 BPCS 又用做 SIS 系统，假设这个阀门在开的状态出现故障就会产生问题，如该阀门也作为一个联锁装置，这时因为 SIS 系统不能够关闭该阀门，从而使得这个安全保护失效。

**B.1.6.3** 对于 SIL 3 级，为了满足安全完整性的要求，BPCS 和 SIS 系统同样分离或者不同分离是通常需要。

**B.1.6.4** 当使用冗余的 SIS 阀门时，这些阀门可以同时接到 BPCS 和 SIS 系统，只要安全审查和安全分析表明这时阀门接到 BPCS 并不会危及 SIS 系统的安全完整性。

**B.1.6.5** 决定阀门要求另外还要考虑的问题有：

- a) 关断要求；
- b) 阀门的可靠性经验；
- c) 阀门出现不安全故障的模式；
- d) 降低阀门的有效性的操作程序（如旁通阀打开）。

**B.1.7 逻辑控制器：**

**B.1.7.1** 对于 SIL 1 级，为了满足安全完整性的要求，BPCS 和 SIS 系统同样分离或不同分离的需要是典型的。

**B.1.7.2** 对于 SIL 2 级，为了满足安全完整性的要求，BPCS 和 SIS 系统不同分离的要求是具有代表性的。只要安全审查和安全分析表明满足安全完整性的要求后，可以使用 BPCS 和 SIS 系统同样分离。

**B.1.7.3** 对于 SIL 3 级，应考虑用 BPCS 和 SIS 系统不同分离来满足安全完整性的要求。

**B.1.7.4** 可能有一些特殊的场合 BPCS 和 SIS 系统是不能进行分离的（如一个燃气透平控制系统就包含控制和安全两者的功能）。当控制和安全两者的功能在同一个装置结合起来时还要考虑的问题有：

- a) 公共元件和软件故障以及它们对 SIS 性能影响的评估；
- b) 安全生命周期内考虑到 SIS 系统修改、维护、测试时整个系统的技术支持和文件支持；
- c) 限制访问系统的编程和组态功能。

**B.1.8 BPCS 和 SIS 系统之间的通信：**

**B.1.8.1** BPCS 和 SIS 系统之间的通信能够增强应用的整个安全性。但是，外部通信特别是 SIS 的写入可能影响 SIS 的安全完整性。必须有准备地确保所有写入正确，不会给系统的安全和操作带来消极影响 [进一步的说明参见 B.1.8.2c) 和 d)]。

**B.1.8.2** BPCS 和 SIS 系统之间的外部通信有下列 5 种基本的方法：

- a) BPCS 和 SIS 系统之间没有外部通信。这种做法对于所有的 SIL 级别都可以接受。
- b) BPCS 和 SIS 系统之间硬线连接的外部通信。这种做法对于 SIL 1 级和 SIL 2 级可以接受，但对于 SIL 3 级需要做额外的安全审查和安全分析。

例如，从一个设备输出模拟量或数字量到另外一个设备的输入。

- c) 从 SIS 系统到 BPCS 系统的只读外部通信。如果经安全审查和安全分析确信不会影响安全功能，这种做法对于所有的 SIL 级别都可以接受，实现安全功能的写保护措施包括但不限于以下几种：

- 1) 硬线开关(或跨接线)限制写入;
  - 2) 在 SIS 的 ROM(只读存储器)中完成安全功能。
- d) 带有写保护安全功能的读取/写入的外部通信。这种做法对于 SIL 1 级和 SIL 2 级可以接受,但对于 SIL 3 级需要做额外的安全审查和安全分析,实现安全功能的写保护措施包括但不限于以下几种:
- 1) 为写入访问限制时间窗;
  - 2) 软件开关(如密码 password)来限制写入访问。
- e) 带有少量或没有写保护安全功能的读取/写入的外部通信。这种做法对于 SIL 1 级可以接受,对于 SIL 2 级需要做额外的安全审查和安全分析,在 SIL 3 级不建议使用这种方法。

## B.2 冗余——同样的或者不同的

**B.2.1** 冗余能够用来提高安全完整性或者改进故障容错。设计者应该确定实现安全等级的冗余需求和确定安全系统中所有部件,包括检测元件、逻辑处理器和终端控制元件等的可靠性要求。

**B.2.2** 其中一个例子是安全系统要求 2 选 1 (1002) 的结构体系,但是要关心谬误跳闸问题。在这种情况下,设计者可以选择 3 选 2 (2003) 的结构体系,这样在没有实质上降低安全完整性的情况下即可以改进可靠性。

**B.2.3** 冗余可适用于硬件和软件(参见 B.10)。

**B.2.4** 对于公共原因故障应进行冗余分析。消除或减少故障源,使用不同的冗余技术是减少公共原因故障的有效办法。公共原因故障的例子有:

- a) 公用仪表检测管堵塞;
- b) 腐蚀;
- c) 硬件故障;
- d) 软件错误;
- e) 动力供应/源。

**B.2.5** 不同的冗余采用不同的技术、设计、制造、软件和固件等,来降低公共原因故障的影响。如果需要不同冗余来满足 SIL (安全等级),就应该采用不同冗余。如果由于采用了不同冗余可能导致使用低可靠性部件,从而不满足系统可靠性要求,不同冗余则不应该被采用。

**B.2.6** 能够用来实现不同冗余的措施包括但不限于下列:

- a) 当不同检测量之间存在已知关系时,使用不同检测量(如压力和温度);
- b) 对于相同的参数采用不同的检测方法(如科里奥流量计和旋涡流量计);
- c) 对于冗余结构体系的每一个通道采用 PES 的不同类型;
- d) 使用地理上的不同(如冗余通信介质的备用路由)。

**B.2.7** 在 SIS 中采用 PES 技术能够保证不同冗余,但需考虑在下列几个方面存在未被检测到的故障:

- a) 硬件;
- b) 制造;
- c) 元件;
- d) 操作系统;
- e) 通信;
- f) 固件;
- g) 软件;
- h) 应用程序;
- i) 环境。

## B.3 软件设计考虑

### B.3.1 内置软件

**B.3.1.1** 内置软件由 PES 供应商提供并且对于应用程序的制备具有明显的代表性。进行应用程序开发之前应先明确下列问题：

- a) 供应商有软件质量计划；
- b) 内置软件修订本版本号是规定好的；
- c) 内置软件修订本版本号与最初批准 PES 用着 SIS 进行分析时的修订本版本号是相同的；
- d) 在新软件版本中所有增加的内置软件功能要进行审查和分析。

### B.3.2 公用软件

**B.3.2.1** 使用公用软件应该坚持和内置软件一样的标准（参见 B.3.1）。可以考虑采用从第三方来的公用软件。如果公用软件包未经 PES 制造商测试和批准，不推荐使用第三方的公用软件进行应用程序开发。

### B.3.3 应用软件

**B.3.3.1** 标准组件型模块化设计在应用软件中是非常可取的，标准组件型模块化设计往往使设计趋于简单、完整。

**B.3.3.2** 如果需要满足系统的安全等级（SIL），应用软件应该包括诊断测试规定。典型的使用看门狗计时器的诊断测试方案在 [参考 C.1] 中举例说明。

**B.3.3.3** 首选使用成熟的和已被证明为公认的工业标准的程序语言。

**B.3.3.4** 编程准则应该建立在设计组中实施统一的风格。软件质量计划的实施可以更加容易发展统一的编程风格。

**B.3.3.5** 为了避免不必要的使得系统难于预知的复杂性和特征，下列问题应该考虑：

- a) 软件应该有明确的顺序和结构，以便确保在任何时候都知道是处在应用软件中的什么位置；
- b) 如果嵌套顺序被使用，嵌套应该限制在尽可能少的层上；
- c) 应用软件的同级评审。

**B.3.3.6** 为检验软件设计满足安全需求技术规格书中确立的每一项要求，要考虑下列问题：

- a) 一个分析证明安全需求技术规格书中确立的每一项要求已在设计中被贯彻；
- b) 安全临界功能设计的同级评审。

**B.3.3.7** 证实应用软件在所有预期的操作条件下都满足安全要求技术规格书中确立的每一项要求，要考虑下列问题：

- a) 测试应该逐步展开，以练习软件超出正常限制的数据、命令、键盘输入和其他动作；
- b) 一个缺陷报告和判别系统应该被执行；
- c) 应用软件应该被测试，以测定存在硬件故障中的软件工作情况。

## B.4 技术选择

**B.4.1** 安全仪表系统（SIS）可以采用电气的、电子的或可程序电子（E/E/PE）的技术。

**B.4.2** 组合技术（如 PE、电气等）的混合方案能够用于开发 SIS。

**B.4.3** SIS 的设计除 E/E/PE 外还可以使用其他技术，如气动的、液压的等等。但这些技术在本标准的范围之外（参见 1.2.9）。

**B.4.4** 用于 SIS 中的电气的技术：

**B.4.4.1** 直接接线系统：

**B.4.4.1.1** 直接接线系统将离散检测元件直接接到最终的控制单元。这种技术只能用在最简单的应用场合。因该系统诊断覆盖率较小，因此验证测试的次数应增加。

**B.4.4.2 电动机械装置：**

**B.4.4.2.1** 电动机械装置包括继电器和计时器。继电器通常使用在简单逻辑功能足够提供所需要的安全逻辑的地方。人们对继电器丰富的操作经验和它们成熟的技术使得这种装置在 SIS 中普遍被接受。

**B.4.4.2.2** 用户有在 SIS 应用中采用电动机械继电器的标准和指南（参考 C.4）。继电器的非安全故障模式能够被量化。

**B.4.4.2.3** 在安全应用中使用继电器的成功用户遵循下面一些简单的指导准则（包括使用一个继电器）：

- a) 有一个良好的工厂实施的跟踪记录；
- b) 在安装时有固有的“故障位置”状态特性（如完全断开时的状态）；
- c) 通过寿命测试发现是可靠的；
- d) 用户批准作为安全应用的；
- e) 适合安装位置所在的环境（如气密的）。

**B.4.4.2.4** SIS 继电器还有其他的属性应该考虑到：

- a) 开/关状态能够容易通过检查触点位置（开或关）获得；
- b) 内部连接逻辑的改变非常困难（要求重新接线）；
- c) 对于工厂工人简单易懂和易于维护；
- d) 作为关键的控制装置是易于识别和安全的；
- e) 故障模式能够隔离以减少共模故障的发生。

**B.4.4.2.5** 继电器逻辑不应该认为是固有故障失效安全型。即使继电器的选择和应用适当，失电时触点可能熔结、弹簧也许没有使开关触点转换至失电的位置。

**B.4.4.2.6** 电动机械继电器逻辑系统应该考虑下列标准：

- a) 在线圈失电或故障时触点打开；
- b) 线圈有重力脱扣或双弹簧；
- c) 触点有恰当的材料和等级；
- d) 安装能量限制负载电阻以防止触点熔结关闭；
- e) 触点的电弧抑制要提供电感负载。

**B.4.4.2.7** 有一些低能量负荷（如 50V 或者更低和（或）10mA 或者更低）要求特殊的触点材料或设计（如密封的触点）以消除触点氧化引起的不可靠操作（如负载脱扣），这里称为湿触点。当使用这样的特殊触点时，要求针对这些触点进行故障分析，以保证设计出一个故障安全型电动机械系统。

**B.4.4.2.8** 电动机械继电器可能不适合在下列场合作为 SIS 应用：

- a) 快速的工作循环引起状态的频繁改变；
- b) 计时器或闭锁功能；
- c) 复杂的计算功能；
- d) 模拟测量；
- e) 大的逻辑应用。

**B.4.4.3 马达驱动计时器：**

**B.4.4.3.1** 马达驱动计时器提供可接受的功能给关键的安全应用场合，如燃烧器清扫计时。许多马达驱动计时器需要一个锁定装置或者适当的限制，以避免篡改危险的设定。马达驱动计时器在时间分辨率上是有限的，不能够处理高的工作循环。

**B.4.5 用于 SIS 中的电子技术：**

**B.4.5.1 固态继电器：**

**B.4.5.1.1** 固态继电器在高的工作循环中使用，并且有能够被识别和量化的不安全故障模式。适当

的设计特点应该增加对这些不安全故障模式的处理。固态继电器一些另外的应用在下面段落中描述。

#### **B.4.5.2 固态计时器：**

**B.4.5.2.1** 固态计时器用在那些复杂程度还没有必要用 PES 的地方。固态计时器技术能够列入阻容 (RC) 电路或者脉冲记数的范畴。RC 计时装置由于重复性差和不安全故障模式可能不适合作为安全应用。注意 RC 电路通常用在脉冲计数计时器的时间设定部分；这一点不排除这些计时器的使用。

**B.4.5.2.2** 脉冲计数计时器，有时称为数字计时器，能够使用许多的方法实现脉冲计数，包括：

- a) 一个线性频率 (50Hz 或者 60Hz)；
- b) 一个电子振荡器；
- c) 一个石英晶体振荡器。

**B.4.5.2.3** 用户批准的安全晶体振荡器 (如石英) 的计时器往往被推荐使用是由于它较高的可重复性和良好的可靠性。

#### **B.4.5.3 固态逻辑器：**

**B.4.5.3.1** 固态逻辑器是指晶体管家族的元件，如互补型金属氧化物半导体 (CMOS)、电阻晶体管逻辑器 (RTL)、晶体管—晶体管逻辑 (TTL) 器和高抗扰性逻辑电路 (HNIL)。这些元件是集成在单机模块、插板模块中，或者高集成、高密度芯片中。它们不同于典型的计算设备，没有中央处理单元 (CPU)。它们按照由相互联系的各种逻辑单元，如与、或、非直接接线技术获得逻辑执行。应该认识到这些系统在故障安全型要求 (如不确定故障模式) 方面有局限性。

**B.4.5.3.2** 固态逻辑器通常与直接接线和继电器设计成一体作为 SIS。除非提供额外的诊断以测试非安全故障模式，固态逻辑器不推荐用于 SIS。PES 有时用来作为诊断工具，使得固态逻辑器系统适合于 SIS。

#### **B.4.5.4 脉冲电子逻辑器：**

**B.4.5.4.1** 脉冲电子逻辑器产生特定的振幅和周期的脉冲。一个脉冲序列被认可为逻辑“真”或“1”，而其他所有信号 (如接地、非规定脉冲、连续的开或关) 是被认可为逻辑“假”或“0”。

**B.4.5.4.2** 脉冲电子逻辑器如果满足本标准注明的要求和用户批准，则能够考虑用在 SIS 中。

**B.4.5.4.3** 脉冲电子逻辑器能够提供提高的安全完整性。但是，PES 设计能提供的功能，如计算能力、改善通信和网络等是脉冲固态系统和电子逻辑器所没有的。

#### **B.4.6 用于 SIS 中的 PES 技术：**

**B.4.6.1** PES 能够是一个可编程序控制器、一个分散控制系统控制器或者一个专门应用型单机微处理器。当使用个人计算机时要慎重，因为它们通常不具备 SIS 应用所要求的安全完整性。

**B.4.6.2** 使用 PES 导致认识故障模式的许多困难，许多故障可能是不安全的。

**B.4.6.3** 下列一些技术能够用来把 PES 的不安全故障模式减少到最小：

- a) 广泛的诊断以检测出隐性故障 (参见 B.9)；
- b) 使用冗余、容错 (如 3 选 2) 和相似的结构；
- c) 对内和对外都使用监视计时器；
- d) 使用带诊断的输出以检测输出模块故障。

**B.4.6.4** 在下面情况时选择 PES 技术作为 SIS：

- a) 有大量的输入输出，或者有许多模拟信号；
- b) 逻辑要求复杂，或者逻辑包括计算功能；
- c) 与 BPCS 要求有广泛的数据通信；
- d) 对于不同的操作要求不同的脱扣点 (如批处理程序应用菜单选择)。

### **B.5 故障率和故障模式**

**B.5.1** 故障率指 SIS 部件内出现故障的平均比率。元件显性故障率可能和隐性故障率有很大不同，

在 SIS 设计中应该考虑这两种故障率和它们的安全含义。故障率受部件的设计、制造质量、安装过程、环境和运行条件等影响（参见 ISA—dTR84.02）。

**B.5.2** 表 B.5.1 和表 B.5.2 列出了在设计 SIS 时应该考虑的一些可能故障。

**表 B.5.1 典型的 SIS 故障形式**

装 置	故 障 形 式	装 置	故 障 形 式
传感器检测元件	与过程隔绝	电动机机械继电器/计时器	接线故障；线圈烧掉；继电器动作顺序失效
	传感器/变送器卡住		计时故障
	上升/下降卡住		触点熔化
	不正确信号		电枢转子卡住
	漂移/标定错误		触点保真性
	噪扰		接线故障
	转换时间错误		噪声/动态故障/错误应答
	转换错误	固态逻辑	门电路（开—关）堵塞/背板故障
	不正确的供电电压		计数器故障
接线/接头	开路/短路		引导装置故障
	接地故障	终端元件	开/关/中间的位置卡住
	噪声		机械装置卡住
安全栅/端子	开路/短路		能源
	接地故障		变换时间故障
	隔绝故障		变换故障
	错误信号		过电压、电流、压力等
外部通信	不可靠的数据	共模	后备（UPS）电源故障
	不正确的数据		欠电压/电流等
	不正确的来源/目的		全部失电
	不正确的信号交换		临时电源波动
	复制来源/目的		温度太高或太低
	不正确的输入/输出寻址地址		腐蚀
	连接失败		电磁干扰
	接收/发送失败		
	响应超时		
	误差修正失败		
	开路或短路电路		
	冗余信道失败		



表 B.5.2 典型的可编程电子故障形式

装 置	故 障 形 式	装 置	故 障 形 式
PES	堵塞位/多位	PES	错误应答 (DMA)
	动态故障/错误应答		总线请求堵塞 (DMA)
	指令执行时间/等待状态/延迟		传送时间错误 (DMA)
	α 代码/宏代码		错误采样时间
	算术逻辑部件 (ALU) 故障		定时寄存器故障
	访问时间等待状态逻辑		计时器故障
	存取时间		超时/超限
	中断请求堵塞		时基故障
	计时堵塞或失败		设定/复位故障
	装置特性 (用户 IC)		中断请求/轮询故障 (计时器)
	堵塞输入/输出位		触发脉冲伪造 (WDT)
	在输入/输出线上错误应答		触发脉冲太早/太晚 (WDT)
	错误的输入/输出线	输入	卡住开/关
	数据流向故障 (I/O)		刻度上限/刻度下限转换故障
	信号太快/太慢 (I/O 卡)		漂移标定
	丢失位/字节/信息		不稳定的输入
	错误的发送器/接收机/信息 (comm)		隔离故障
	超时/多点冲突		线性化/补偿
	死锁 (comm)	输出	卡住开/关/转换故障
	奇偶发生器故障		刻度上限/刻度下限
	框架缺陷/缓冲器超限		漂移标定
	堵塞直接存储器存储		不稳定的输出
	错误应答 (DMA)		隔离故障
	输入/输出通信失败		线性化/补偿

## B.6 结构

**B.6.1** SIS 体系结构的选择应是在安全生命周期的概念设计步骤中完成。结构主要影响 SIS 的整个安全完整性，也会影响 SIS 的可靠性（谬误跳闸的可能性）（参考 C.3）。

**B.6.2** 涉及决定 SIS 体系结构的一些行为是：

- 得电跳闸或者失电跳闸设计的选择；
- 对于 SIS 的检测元件、逻辑控制器以及终端控制单元采用同样的或者不同的冗余的选择；
- 对于动力源和 SIS 动力供应的冗余选择；
- 操作员界面部件（如 CRT、警报信号器、按钮）和它们与 SIS 连接方式的选择；
- SIS 与其他子系统（如 BPCS）的通信界面和它们的通信方式（如仅有读入或者读/写）的选择。

**B.6.3** SIS 可以利用的体系结构（如 2003 检测元件、1001 逻辑处理器、1002 终端控制单元）可以

从不同原因上来决定：

- a) 在同样的 SIS 中 SIL 等级；
- b) 测试要求；
- c) 设备可靠性和故障形式；
- d) 用户界面。

**B.6.4** 典型的可以满足 SIL 功能要求的体系结构包括：

SIL1——一个 1001 体系结构带有单个检测元件、单个逻辑控制器和单个终端控制单元。

SIL2——要求更多的诊断，通常要求包括检测元件和逻辑控制器冗余，根据需要终端控制单元也要求冗余。

SIL3——通常需要的两个分开且不同的 1001 配置，每一个配置带有它们自己的检测元件、逻辑控制器和终端控制单元。在 1002 表决方案中两个 1001 配置相连。不同的分离、冗余和彻底的诊断能力是一个 SIL3 系统要考虑的重要的方面。

用户必须决定系统元件的故障率、诊断覆盖范围、测试时间间隔、冗余等，并且要评估每一个特定的 SIS 以证实它们的功能（详见 ISA—dTR84.02）。

## **B.7 动力源**

动力源包括但不限于电动源、气动源（如仪表风）和液压力源。接地编排在本节电动源之后。

### **B.7.1 电动源**

**B.7.1.1** 电动源的设计应该满足应用场合的安全完整性和可靠性要求。

**B.7.1.2** 电动源冗余经常地被用作改善 SIS 的可靠性，尽管失电跳闸应用场合可能不需要冗余来满足安全完整性要求。对于得电跳闸应用场合，通常要求电动源冗余来满足安全完整性要求。

**B.7.1.3** 电动源冗余能够用一个带自动切换功能的交流源、一个不间断电源（UPS）、或者交流源的后备电池来提供。当切换到交流源时，设计上的考虑包括：

- a) 在对 SIS 操作的影响前进行故障的探测；
- b) 切换到后备电源不影响 SIS 操作；
- c) 能够维修 UPS 或者电池而不影响 SIS 操作；
- d) 将公共原因故障减到最少。

**B.7.1.4** 考虑提供动力源诊断，不允许 SIS 启动，除非所有动力源可利用。

**B.7.1.5** 电子和可编程电子的 SIS 常常包括把电源转换成供内部使用的低电压电源。动力源冗余应满足应用场合的可靠性要求。

**B.7.1.6** 电子和可编程电子的 SIS 特别对电气噪声（如无线电通信频率影响或电磁影响）更加敏感。应采用屏蔽、良好的接线方式（参见 B.13）和适当的接地（参见 B.7.2）。

**B.7.1.7** 电子和可编程电子的 SIS 有比电气的 SIS 低的绝缘击穿电压等级。因此，可能要求额外的浪涌保护。

**B.7.1.8** 可编程电子的 SIS 可能与电子的 SIS 或者电气的 SIS 相比，要求电源谐波畸变更低、更严格。

**B.7.1.9** 输入/输出（I/O）可以采用分离的电源配电和各自独立的保险丝，从而将由于一个接线故障引起的共同故障减小到最小。这些保险丝应与上游保险丝互相配合，以确保如果一个保险丝烧断对系统功能的影响最小。

**B.7.1.10** 对交流电源考虑的检查应包括：

- a) 电压和电流范围，包括冲击电流；
- b) 频率范围；
- c) 谐波；

- d) 非线性负载;
- e) 交变时间;
- f) 过载和短路电流保护和互相配合;
- g) 雷电保护;
- h) 瞬变现象诸如尖峰信号、浪涌、断路和电气噪声的保护;
- i) 欠电压的保护;
- j) 过电压的保护;
- k) 接地。

#### **B.7.1.11 对直流电源考虑的检查包括:**

- a) 电压和电流范围包括冲击电流;
- b) 非线性负载。

#### **B.7.2 接地**

**B.7.2.1** 接地在 E/E/PE 技术中,是确保人身安全和设备性能良好的关键。本节仅考虑在 SIS 应用中的电压(典型的交流 240V 或更低,直流 125V 或更低)。

**B.7.2.2** 当从电气转到电子和从电子转到可编程电子时,接地变得有更多限制性。因此,电气设备的接地相对于电子或者可编程电子设备来说,在一个接地系统的设计上可能更易于实现,电子设备的接地相对于可编程电子设备在一个接地系统的设计上可能更易于实现。可编程电子设备中安装一个按电气标准设计的接地系统可能是不适当的。

**B.7.2.3** 对于不接地系统,考虑使用适当的接地故障监测继电器和报警器。

**B.7.2.4** 注意电气或者电子技术将可编程电子并入它们的设备中通过改善通信、诊断、人机界面等提高性能。在这些情况下,接地按可编程电子接地处理,除非供货方安装指南规定一个不同的方法。

**B.7.2.5** 接地系统应该满足制造商的推荐作法。如不一致应该进行安全检查和他分析。

#### **B.7.2.6 接地需要考虑的检查包括:**

- a) 腐蚀保护;
- b) 阴极保护;
- c) 避雷针保护;
- d) 接地平面(参考 C.16);
- e) 凸起的地板接地;
- f) 静电保护;
- g) 屏蔽接地;
- h) 单点接地;
- i) 测试接地;
- j) 本质安全栅接地;
- k) 接地端子可用性。

#### **B.7.3 气动源**

**B.7.3.1** 仪表空气(或者其他气体)典型的是用在终端单元如控制阀上。电磁阀用作电/气继电器。仪表空气应该是经过过滤、干燥和连续监测,确保维持适当的压力,系统应该有备用,达到所需的无故障时间以满足可靠性要求。

#### **B.7.3.2 仪表空气检查清单:**

- a) 压力;
- b) 湿度;
- c) 杂质;
- d) 润滑油(在需要的地方);

e) 容量。

#### **B.7.4 液动力源**

**B.7.4.1** 液动力源典型的是用在要求高推力的地方，如很大的阀门。

**B.7.4.2** 液动力源检查清单：

- a) 压力；
- b) 容量；
- c) 杂质；
- d) 液体特性。

#### **B.8 公共原因故障**

**B.8.1** 公共原因故障可以由单个（非冗余）元件或者冗余元件中的系统错误引起。

**B.8.2** 公共原因故障的一些例子包括：

- a) 技术规格错误；
- b) 硬件设计错误；
- c) 软件设计错误；
- d) 人机界面设计问题；
- e) 环境过度超限（过高/过底温度—湿度—压力、腐蚀）；
- f) 单个元件：公用工艺管嘴，[参考 C.1] 中图 5.11，公用（电缆）管道，单个电源，单个现场装置等；
- g) 工艺腐蚀或者堵塞；
- h) 振动；
- i) 维护（如工具、步骤、标定、培训）；
- j) 对于误操作的敏感性（如培训、步骤、在非正常压力的行为）。

**B.8.3** 设计时使用适当的故障避免方法，可以减少常见故障或者系统性错误。考虑使用的方法有：

- a) 提供给供货商应用的技术规格信息（如规则标准、型号）；
- b) 验证；
- c) 不同的分离；
- d) 不同的冗余；
- e) 相同的冗余；
- f) 相同的分离。

**B.8.4** 许多独立功能的 SIS 可以共享外围设备、操作柜、操作员界面、维修/工程师界面。这些独立的系统仍然需要独立动力与逻辑控制器以实现测试维修。在做系统整体规划设计时应该考虑这些因素的影响。

#### **B.9 诊断**

##### **B.9.1 总则**

**B.9.1.1** 诊断是周期性地和自动地执行测试以便检测到阻碍 SIS 对指令进行响应的隐性故障（见 ISA—dTR 84.02）。

**B.9.1.2** 可能出现的各种各样的故障类型包括在表 B.9.1 中。

**B.9.1.3** 在系统中隐性故障可能阻止 SIS 一个指令应有的响应。它可以是单通道系统中第一故障或者是多通道系统中故障组合。因此不仅发现危险性故障是重要的，而且在潜在危险故障聚集前发现也是重要的。

表 B.9.1 故障类型

故障类型	例子
立即使 SIS 丧失响应指令能力的故障（危险的故障）	一个关键性的输出点粘住或粘开
与其他故障结合使 SIS 丧失响应指令能力的故障（潜在的危险故障）	一个关键性的输出点诊断没有执行
没有指令但触发了 SIS 一个安全响应的故障	由于元件故障造成的谬误跳闸
没有影响到 SIS 响应指令能力的故障（良性的故障）	烧坏，没有关键的 LED 指示

**B.9.1.4 故障能够导致两种类型的失效：**

- a) 随机的失效，元件自然产生的失效；
- b) 系统性的失效（或错误），在设计或执行中一个隐藏的故障。

**B.9.1.5 硬件倾向于随机的失效，但是也可能有系统性失效（不正确的定时、元件使用超过它们的技术范围等等）。****B.9.1.6 软件一般没有随机失效，但系统性失效的可能性很大。一旦系统性故障变成显性，要能够被纠正并且消除。****B.9.1.7 随机故障是自然发生的，根据故障持续的时间，可能有两种情形：**

- a) 固定的随机故障持续直到它们被维修；
- b) 在某些情况下，动态的随机故障（串音、热的故障等）产生又消失。

**B.9.2 诊断测试****B.9.2.1 诊断可以使用各种方法或它们的组合实现，包括：**

- a) 硬件完整性监测（如热电偶的阻抗监测）；
- b) 购买的 SIS 设备中提供的自动内置测试（如输入/输出模块自测）；
- c) 把自动测试并入到应用程序特殊设计中（如通过输入点读回输出信号）；
- d) 看门狗计时器、信号比较、尾端监测等；
- e) 比较冗余信号。

**B.9.2.2 对故障的固有安全响应可以替代对该故障诊断的需求。但所谓“安全”设计的元件并不总是产生 SIS 的安全响应，因为这是应用特例。****B.9.3 诊断覆盖范围****B.9.3.1 特定的诊断技术在检测所有可能的故障时，其有效性通常都小于 100%。对于描述的故障可使用估算的诊断“有效性”。****B.9.3.2 改进 SIS 的诊断覆盖范围有助于满足安全完整性级目标的要求。表 B.9.2 中列出了可以被诊断覆盖的特殊故障模式。该表或相同故障模式的表可用来确定要求的诊断覆盖范围的区域。****B.9.3.3 危险的和潜在的危险故障（如 CPU/RAM/ROM 故障）将几乎抑制整个数据的处理，因此比单个输出点故障影响范围更远。这种类型故障诊断覆盖范围的要求因此更加严格。另外，高故障率的故障类型必须更加可靠的去检测。此外，故障模式的可检测能力必须考虑（应该随时使用简单方法检测故障）。****B.9.3.4 对于每种实现的诊断，应该确定如下内容：**

- a) 测试时间间隔；
- b) 故障发现时引起的动作；
- c) 上述两项应该满足安全技术规格书要求。

**B.9.3.5 当某些诊断没有内置在厂商提供的设备中时，可在系统或应用级别实现适当的诊断。****B.9.3.6 诊断可能不能够检测到系统错误（像软件瑕疵）。但可采用适当的预防措施，检测可能的系统性故障。**

表 B.9.2 对于可编程电子设备的诊断测试

项目	硬 件		软 件	
	可能的原因	检 测	可能的原因	检 测
数据	芯片错误	硬件故障测试	错误的恒定值	—
地址	—	—	变址	硬性限定检查
时间	错误的电路	—	重要事件	重要事件查证
	技术规格以外的元件	—	时序安排	时序安排监测
处理	表决策故障	随机表决策测试	运算法则	确定
				真实性检查
				反向
				计算
				差异

## B.10 现场设备

### B.10.1 总则

**B.10.1.1** 许多引起的现场设备公共原因故障可以通过适当地采用设备冗余和（或）使用不同的设备来避免。例如，在某一应用场合要求采用具有不同工作原理或由不同制造商提供的冗余传感器。

**B.10.1.2** 两个模拟传感器，两个开关量传感器（开关），或两类传感器中各选一个。如果选择一个模拟传感器和一个开关量传感器以实现多样性，相对于采用两个模拟传感器的情况，此种组合将丧失可连续地对信号进行比较的优点。开关量设备操作的正确与否，仅可通过测试或检查相应过程所期望事件的发生来进行核实。如果选择两个模拟设备，它们能够进行连续的比较。这种比较大大地减少了平均故障探测时间，因此提供了更有效的保护。

**B.10.1.3** 下面有关现场设备的 SIS 的考虑可提高现场设备的应用：

- 在系统操作过程中连续比较冗余传感器（如在产生不可接受的偏差时报警或关闭）；
- 比较流量或其他有关的变量以调整阀位；
- 在每种关断情况下，比较已知关断条件下的传感器读数并进行传感器之间的相互比较（如用这些比较作为下次启动的许可条件；这将减少现场设备平均故障检测时间；这也适用于用限位开关监测阀位的情况）；
- 如果安全仪表系统具有将在当前现场传感器所得的不正确值显示为最后一个正确值的内在特性，则此特性应该被废除（对于应用 SIS 的场合，信号应允许达到其极限值）；
- 当末端的执行元件不能达到所要求的状态时，进行反馈报警；
- 如果现场设备在没有得到 SIS 的操作命令情况下而改变状态，应报警；
- 厂商给出的设备平均故障间隔时间（MTBF）；
- 故障种类的预知性；
- 在同样的位置性能能保持很长一段时间；
- 避免在超出传感器测量精度范围时进行测量（举例来说，超传感器的精度/量程比要求，例如，确认流量为零的场合，不能用流量传感器来测量流量）；
- 标识（类别、颜色代码等）；
- 对于分析测量，应尽量设计能提供将分析读数与有关的基本测量量，如压力和温度等等相比较的系统。

**B.10.2 现场设备故障模式及相应的检查方法**

**B.10.2.1** 从本质上来讲,所有现场仪表都有三种故障状态——仪表的两个极端状态和中间某状态。

- a) 传感器: 上限、下限、刻度范围内。
- b) 电流/电压报警跳闸: 电流/电压报警跳闸是将电流或电压(如 4mA~20mA 或 0VDC~10VDC)模拟输入信号转换为离散型输出信号。跳闸设定值现场可调。这些开关具有非安全故障模式,应该进行适当的分析和设计特点研究以确保其安全操作。
- c) 阀门: 全开、全关、部分打开。
- d) 继电器: 线圈不动作、触点保持在它们的“正常”位置、触点熔接闭合、触点磨坏导致高阻抗/限制电流量、烧毁电枢。

**B.10.2.2** 已知上述故障模式,考虑选择具有下述固有特性的元件: 能将设备置为可检测到的其故障模式发生概率高的一种极端状态。

**B.10.3 传感器选择标准**

**B.10.3.1** 选择传感器时,应考虑:

- a) 模拟设备与离散设备相比,优选模拟设备;
- b) 在可能的场合,尽量通过测量均可指示同一异常情况的不同的变量来实现冗余和(或)多样性;
- c) 认真检查可能影响取压管线的填充/排空的过程/环境条件;
- d) 检查密封模盒中的密封液,密封液被用于提供隔离、防冷凝及聚合,以避免引起错误的读数;
- e) 被选择用来实现多样性的设备应有足够的可靠性以满足系统可靠性要求,否则考虑实现多样性的替代方法;
- f) 对于工厂维护机构不能维修的设备应该认真权衡后加以选用。

**B.10.3.2** 在工艺过程和用于 SIS 的传感器之间应尽量少的使用切断阀。每一要求有工艺切断阀的传感器都应有专用的连接和阀门( [参考 C.1] 中图 5.11)。

**B.10.4 应用终端元件的考虑因素**

**B.10.4.1** 在将阀门用作最终控制部件时考虑的因素包括:

- a) 阀门的开/关速度;
- b) 切断差压;
- c) 泄漏(切断等级要求);
- d) 阀体和执行器的防火性能;
- e) 同一开度,长时间工作的性能;
- f) 在满足要求的场合下,可考虑使用调节作用的控制阀作为终端阀门元件之一,因为控制回路的操作证实了这种阀并不会卡死在一个位置;
- g) 实现多样性时不能降低可靠性;
- h) 材料的适宜性/可比性;
- i) 认真权衡工厂维护机构不能维修的设备的选用;
- j) 故障位置的考虑;
- k) 阀位指示。

**B.10.4.2 电磁阀:**

**B.10.4.2.1** 在应用电磁阀时的考虑因素包括:

- a) 当选择电磁阀时,应考虑温度、电压等级、区域划分和负荷等因素;
- b) 供气压力最大或最小对电磁阀影响;
- c) 确保电磁阀的尺寸计算正确;
- d) 具有可调整的流量通道,以便在对电磁阀进行不正确的调整时,具有使 SIS 功能失效的可能;

- e) 电磁阀安装于阀门定位器与阀门之间;
- f) 有些电磁阀对安装位置敏感——细节安装要求;
- g) 电磁阀放空口应有保护装置以防堵塞、灰尘、昆虫、结冰等等。

#### **B.10.4.3 马达启动器:**

**B.10.4.3.1** 通常不使用冗余的马达启动器,可采用控制回路中的触点冗余。辅助触点被用来给安全仪表系统提供反馈信息以确认启动器的状态(位置)。

#### **B.10.5 输入信号调整器和输出放大器**

输入/输出接口设备为专用的固态继电器。它们具有非安全故障模式,应被确定和量化。在这些设备被批准用于 SIS 前,应增加适当的设计特点以处理这些非安全故障模式。

固态逻辑系统或 PES 要求使用输入/输出接口作为信号调整器。输入信号调整器接受适于工厂级操作强度(如 120V, 48V, 24V, 4mA~20mA)的传感器信号。在固态 SIS 中使用输入/输出接口的目的是隔离 SIS 中的低能逻辑系统(典型的直流低电压)与高能现场系统(典型的信号等级是 120VAC 和 24VDC)。

在逻辑系统中采用低能信号等级以便获取高的信号处理速度。在现场设备中采用高能信号等级是为在长距离传输中保持高的信噪比和确保作为输入设备的离散型传感器的触点拥有足够的动力(电压和电流),以提供适当的触点湿接能力。输出放大器接收来自自固态电路或 PES 逻辑解算器的低能信号,并将它转变为适于驱动终端元件(如电磁阀)的信号。

### **B.11 用户界面**

对于与安全相关的 PES 的用户界面是指操作员界面和维护/工程师界面。

#### **B.11.1 操作员界面**

被用来实现操作员与 SIS 之间信息交流的操作员界面包括:

- a) 视频显示器;
- b) 具有灯、按钮、指示器和开关的仪表盘;
- c) 报警器;
- d) 打印机;
- e) 上述设备的任意组合。

##### **B.11.1.1 视频显示器**

**B.11.1.1.1** 视频显示器可同时具有安全和过程控制功能。基本过程控制系统(BPCS),或其他基于计算机的控制系统,通过标准的操作员显示可给 SIS 提供独立的操作员界面。

**B.11.1.1.2** 展示给操作员的 SIS 的数据应以所要求的速率更新和刷新,从而保证在紧急情况下操作员与 SIS 之间的通信,满足安全响应要求。

**B.11.1.1.3** 与 SIS 有关的显示应被清晰地标识,以避免在紧急情况下信息模糊不清或造成操作员将信息混淆的可能性。操作员应能方便地进入 SIS 显示画面,最好采用通过单键敲击或触摸屏进入显示层的方式。

**B.11.1.1.4** 在每一屏的显示画面中应有充足的信息,以便将危险的信息迅速地传达给操作员。显示的一致性是非常重要的。在与安全无关的显示中应使用相同的访问方法、报警习惯和显示体系。

**B.11.1.1.5** 显示画面布置是非常重要的。在一幅显示画面中信息太多可能会导致操作员读错数据并采取错误的动作。利用颜色的变化、闪光指示和合适的间隔来使操作员获取重要信息并减少误读信息的可能性。信息一定要清晰、简练且明确。

**B.11.1.1.6** 操作员界面和有关的系统(例如分散式控制系统)可用来实现对与安全有关的事件的自动记录和报警功能。要记录的内容包括 SIS 事件(如跳闸和预跳闸发生),SIS 的程序何时被修改和诊断等。



**B.11.1.2 仪表盘**

**B.11.1.2.1** 仪表盘应布置在便于操作员操作的位置。

**B.11.1.2.2** 仪表盘的布置应确保盘上按钮、灯、仪表和其他信息的布置不会使操作员将其搞混。将用于关断不同工艺单元或设备的、外观上相同的关断按钮布置在同一组，可能会导致操作员在紧急情况下由于精神压力而关断不应关断的设备。应将这些关断按钮分开布置并醒目地标出其功能。应提供测试所有指示灯的方法。

**B.11.1.3 打印机**

**B.11.1.3.1** 与 SIS 相连的打印机不能因故障、关闭、脱机、缺纸或运转不正常而影响 SIS 的安全功能。

**B.11.1.3.2** 连接到基本过程控制系统的 SIS，可以利用基本过程控制系统的设施，记录和打印与安全有关的信息。

**B.11.1.3.3** 因打印机可以提供标有仪表位号和时间日期的报表，因此打印机在提供事件发生顺序信息、诊断和其他与安全有关的事件和报警时间方面是非常有用的。应提供公用的报表格式。

**B.11.1.3.4** 如果打印是基于缓冲操作（信息先存储起来，然后根据需要或定时打印出来），那么缓冲区应该足够大以确保信息不会丢失，且在任何情况下，不能因缓冲区内存储空间已满而损害 SIS 的功能。

**B.11.2 维护/工程师界面**

**B.11.2.1** 维护/工程师界面包括提供编程、测试和维护 SIS 的界面设备。界面用于执行下列功能：

- a) 系统硬件组态；
- b) 应用软件开发、文件归档和下载到安全仪表系统、逻辑控制器；
- c) 访问应用软件以对其进行修改、测试和检测；
- d) 了解安全仪表系统的资源和诊断信息；
- e) 改变安全仪表系统的安全等级以及访问应用软件变量。

**B.11.2.2** 维护/工程师界面应能显示所有 SIS 所有元件（例如输入/输出模块、处理器等等）的操作和诊断状态以及构成元件之间的通信情况。

**B.11.2.3** 维护/工程师界面应能提供将应用程序拷贝到存储媒体上的手段。

**B.11.2.4** 用户认可的个人计算机可用作维护/工程师界面。

**B.12 安全****B.12.1 总则**

**B.12.1.1** 应提供控制访问 SIS（包括逻辑控制器、SIS 维护界面、测试和旁路功能、SIS 报警、传感器和终端元件）的方法。访问保护可以是一种保险箱的形式，“只读”通信、访问密码、口令、管理程序等等。

**B.12.1.2** 应用这些选项的指导，见 [参考 C.1] 中 6.1.9。

**B.12.2 例外**

对下列操作的保护超出本附录的范围：

- a) 恶意的修改；
- b) 修改有误。

**B.12.3 对 PES 的补充考虑**

**B.12.3.1** 通过综合应用逻辑和主机操作，可以为影响安全操作性能的任何 SIS 的用户接口设备提供访问控制和保护：

- a) 适于与操作员交互作用的参数应可访问；
- b) 经过审查后可在线修改的参数应置于访问控制保护之下；

c) 修改后需经确认的参数或功能仅可置为离线可访问方式。

**B.12.3.2** 限制访问 SIS 操作模式、程序和数据的能力应是安全仪表系统所必备的特性。

### **B.13 接线**

**B.13.1** 接线应符合制造商的建议及 NEC 的要求。与有关要求不一致的，需进行安全审查和分析。

**B.13.2** 考虑通过下列措施以强化接线作业规程：

- a) 取消多个回路共用同一公共线的接法；
- b) 增加电路以实现更好的隔离；
- c) 增加保险丝以隔离公共原因故障；
- d) 实现测试功能；
- e) 消除接地回路问题；
- f) 将用于 SIS 的端子与其他用途端子分开。

**B.13.3** 对于电子或可编程电子 SIS 的额外考虑包括：

- a) 为防电磁干扰选用双绞信号线（参考 C.7）；
- b) 用于防射频干扰的屏蔽和排扰线，通常在电源侧接地；
- c) 用于防电磁干扰和雷击的总金属护罩（如电缆铠装）或电缆通道（如电缆托架、电缆槽、电缆套管）应在其两端都接地，且应根据距离长短，在其间进行多点接地；
- d) 不同能级的电缆应分开敷设，以避免串扰和辐射噪音干扰；
- e) 恰当的电涌保护；
- f) 不同类型的接地间应进行隔离（如光纤）；
- g) 数据通信电缆的规格和屏蔽应符合制造商推荐要求；
- h) 机柜内接线应妥善布置以减小电气噪音干扰和高温。

**B.13.4** 电子和可编程电子逻辑控制器使用内部低能级逻辑信号。在屏蔽的控制器柜外使用低能级逻辑信号是不合适的。

**B.13.5** 电子和可编程电子逻辑控制器可能要求采取更严格的接线方式，以防止因电感或电容耦合而导致输入信号的错误变化。

**B.13.6** 因漏电流会引起终端控制单元误动作，当使用固态输入或输出时应谨慎。

### **B.14 文件**

**B.14.1** 可用来实现 SIS 的文件包括：

- a) 安全要求规格书；
- b) 应用逻辑；
- c) 设计文件；
- d) 调试预启动认可试验程序；
- e) SIS 操作程序；
- f) SIS 维护程序；
- g) 功能测试程序；
- h) 变更文件的管理；
- i) 定性的或定量的确认 SIS 符合 SIL 的证明文件。

注：文件并不是都必须都需要提供。

**B.14.2** 应用程序备份：

**B.14.2.1** 备份技术能使整个系统尽可能快的恢复操作。这些技术包括下列各项之一或多项：

- a) 拷贝到可移动的存储媒体，例如拷贝至可拷贝回系统的磁带或磁盘；

- b) 拷贝到可移动的能替代损坏的 PES 的磁盘的存储媒体;
- c) 拷贝到用作备份的在线设备上 (如磁盘);
- d) 与其他数字系统的通信连接。

**B.14.2.2** 应考虑对由应用软件积累的用于生成报告、记录和趋势的数据进行独立备份。

#### **B.15 功能测试时间间隔**

关于功能测试的要求参见 9.7。下面是一些用来确定功能测试时间间隔的准则。

**B.15.1** 功能测试的频率应符合适用的制造商的建议和良好的工程惯例。如果以前的操作经验表明需要的话, 应进行更频繁的功能测试。

**B.15.2** 应选择功能测试时间间隔以达到安全完整性级别 (SIL)。

**B.15.3** ISA-dTR84.02 举例说明了各种确定功能测试时间间隔的方法。

附 录 C  
(资料性附录)  
参考资料

注：本附录不是本标准的强制要求，仅供参考。

——使用最新版的参考资料。

——如果资料间相矛盾，优先采用 ISA-S84.01。

——在文中及索引中，下列参考资料用参考资料编号引用。

美国化学工程师学会 (AIChE)

[参考 C.13] 化学过程定量风险分析指南，纽约，1989

[参考 C.14] 危险评估程序指南，纽约，1985

[参考 C.1] 化学过程安全自动化指南，纽约，1993

联系地址：AIChE

345 East 47<sup>th</sup> Street

New York, NY10017 电话：(212) 705-7657

CHEMETICS 国际公司

[参考 C.15] 危险和操作性研究介绍，Knowlton, R.Ellis, 1988

联系地址：Chemetics International Company

Chemical Technology Division

1818 Corwall Avenue

Vancouver BC V6J 1C7

Canada 电话：(604) 734-1200

化学工业学会

[参考 C.15] 危险和操作性研究指南，伦敦，1977

联系地址：Chemical Industries Association

King's Buildings

Smith Square

London SW1P 2JJ

England 电话：44718343399

国际电工委员会 (IEC)

[参考 C.8 和参考 C.9] IEC1508-1995 草案出版物第 1 部分~第 7 部分，电气/电子/可编程电子安全相关系统的功能性安全

注：IEC1508 草案出版物正在编制中；可与贵国的委员会联系获得更多的资料。

联系地址：IEC

P.O.Box 131

3, rue de Varembe

1211 Geneva 20

Switzerland 电话：41227340150

电工和电子工程师学会 (IEEE)

[参考 C.7] IEEE518—1982, RA—1990 减少从外部进入控制器的电噪声电气设备安装指南

联系地址: IEEE

P.O.Box 1331

445 Hose Lane

Piscataway, NJ 08855 - 1331 电话: (800) 6784333

美国仪表学会

[参考 C.2] ISA - dTR84.02 - 1996 用于安全场合的电气 (E) /电子 (E) /可编程电子 (PES) 系统 安全完整性评估技术

注: dTR 84.02 正在编制中; 与 ISA 联系

[参考 C.6] ISA - S91.01—1995 工业生产过程对维护安全起决定作用的紧急关断系统和控制的标识

[参考 C.3] 控制系统可靠性技术的评估及应用, Goble, W M, 1992

联系地址: ISA

P.O.Box 12277

67 Alexander Drive

Research Triangle Park, NC 27709 电话: (919) 990 - 9200

MCGRAW - HILL 公司

[参考 C.16] 科学技术术语字典, 1993 年第 5 版

联系地址: McGraw - Hill, Inc.

1221 Avenue of the Americas

New York, NY 10020 电话: (800) 262 - 4729

美国防火协会 (NFPA)

[参考 C.5] 美国国家电气规程, NFPA70, 1993

联系地址: NFPA

P.O.Box 9101

One Batterymarch Park

Quincy, MA 02269 - 9101 电话: (617) 770 - 3000

保险商实验室公司 (UL)

[参考 C.4] 安全、工业控制设备标准, UL 标准 508—1989 (第 15 版)

联系地址: UL

333 Pfingsten Road

Northbrook, IL 60062 电话: (708) 272 - 8800

英国原子能权威 (AEA 技术)

[参考 C.10] 工业生产过程中风险控制和仪表保护系统, Warrington, UK, 1980

联系地址: UK Atomic Energy Authority

Safety and Reliability Directorate

Wigshaw Lane

**SY/T 10045—2003**

Culcheth Warrington WA3 4NE  
England 电话: 4471925254486

美国联邦法规规程 (CFR)

[参考 C.11] 高危险化学品、爆炸物、爆破剂的过程安全管理, 29 CFR 1910.119—1992 (最终章程: 1992.2.24)

[参考 C.12] 防止化学药品意外泄漏的风险管理程序, 40CFR Part 68 (推荐章程: 1993.10.23)

联系地址: U.S. Government Printing Office  
Superintendent of Documents  
Washington, DC 20402 电话: (202) 512-1800

## 附 录 D

### (资料性附录)

### 举 例

注：本附录不是本标准的强制要求，仅供参考。

#### D.1 范例介绍

本例用于帮助使用者如何使用本标准设计安全仪表系统 (SIS)。本章以 KIS2 公司工艺缓冲罐维持液位为例，KIS2 公司针对此容器进行的过程危险分析 (PHA) 结果作为本例的输入。

本附录中的参考资料用于阐明 SIS 的设计思路和本标准每一步间的关系。标准和附录的参考资料放在 ( ) 中，本标准的强制要求用斜体表示。有必要完整阅读整个附录以便理解所有设计内容。

由于一个高度完整的安全设计要求有大量详细的资料，因此本例做了一些简化。本例中特定的设计并不反映某一公司的实例，也不是惟一的选择。本例确为设计者如何使用本标准提供指导。

期望每个公司都有各自的使用指南，描述解决各自具体问题的方法。无论采用何种方法，最终设计均应满足安全完整性级别 (SIL)。

本附录中的图及指南只是概括性的要求，没有提供规定、设计、安装和维护 SIS 必要的细节。

#### D.2 安全生命周期 (图 4.1)

本例回顾安全要求规格书的编制 (第 5 章)、涉及 SIS 概念设计 (第 6 章)、简要涉及详细设计 (第 7 章)。随后的功能 (如调试、预启动认可试验、维护等) 没有涉及，除非与 SIS 设计有关。

#### D.3 安全要求规格书

##### D.3.1 输入要求 (5.2)

编制安全要求规格书需要从过程危险分析 (PHA) 或过程设计组得到如下资料。

##### D.3.1.1 过程信息描述 (5.2.1)

每个需要 SIS 的潜在危险事件的过程信息描述 (动态、传感器、终端元件等等) (参考 C.6)。

图 D.1 所示的过程，罐内装有热水含有可燃有机物和其他危险化学制品。

压力罐中的液位必须控制。液位由液位变送器 (LT-1) 检测并传到控制器 (LC-1)，控制器输出 4mA~20mA 信号至电/气转换器 (I/P-1) 控制调节阀的位置。压力罐配有安全阀，防止由于加注过度或火灾引起超压。安全阀直接向大气排放。

如果安全阀排放，由于罐中含有危险化学制品，喷射物会引起严重的人员伤害。此外，由于流体是易燃的，可能会引起火灾或爆炸，也会造成严重的人员伤害。

PHA 组已发现两种可能引起罐超压的原因：

- a) 由于管线中有异物，LV-1 处于故障开状态；
- b) LT-1 故障，指示低液位，控制器打开 LV-1。

尽管使用的仪表 (LT-1, LC-1 和 LV-1) 在以往是可靠的，PHA 组认为由于一些安全问题，应增加安全保障以减小风险。

一种选择是去掉安全阀。但这一选择是 ASME 规范所不允许的，同时可能由于外部火灾引起罐超压，造成灾难性事故。另一选择是在安全阀管线上安装一收集罐，设置一报警指示罐中有液体存在，同时表示罐 1-101 有溢流。在这种场合，PHA 组非常关注收集罐的污染、溢流管线的阻塞，同时认为收集罐也会溢流。这种选择被放弃了。因为安全本身不是简单的和 (或) 会产生其他安全问题，因此安装 SIS。

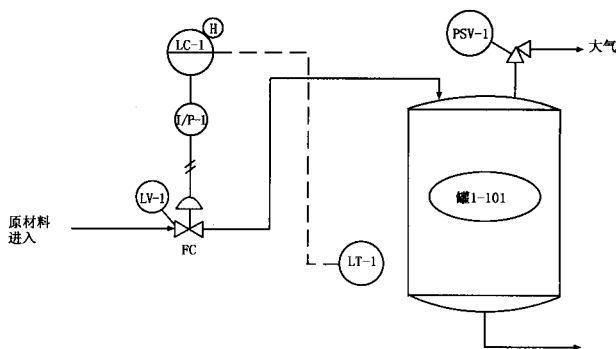


图 D.1 基础过程控制方案

**D.3.1.2 每个安全功能的安全完整性级别 (5.2.2)**

PHA 组同意本例中的 SIS 应设计成 SIL 2 级。

**D.3.1.3 过程公共原因故障考虑 (5.2.3)**

设计组应了解下列公共原因故障可能性：

- 化学药品可能会粘附在液位传感器上，应考虑选择最好的传感器防止故障出现，以便不会形成粘附或将粘附减少到不影响液位传感器工作的水平；
- 应正确选择阀门，防止出现上述同样问题。应考虑使用通径球阀。

**D.3.1.4 规则要求 (5.2.4)**

由于本过程使用大量的危险化学品药品，SIS 应要求遵循 OSHA 29 CFR 1910 (参考 C.11)。

**D.3.2 安全功能要求 (5.3)****D.3.2.1 过程的安全状态**

过程的安全状态是切断所有进罐 1-101 的原材料。

**D.3.2.2 SIS 的过程输入及关断点 (5.3.2)**

当液位达到 90% 时，关断罐的所有入口。

**D.3.2.3 正常操作范围 (5.3.3)**

正常操作范围为罐液位的 20%~80% 之间。

**D.3.2.4 SIS 的过程输出及动作 (5.3.4)**

需要冗余 (1002) 关断阀，其中一个阀门与 BPCS (LV-1) 共用，两个阀门均故障关闭。

**D.3.2.5 过程输入与输出的功能关系，包括逻辑、算术功能及任何要求的功能 (5.3.5)**

对于复杂控制系统的功能关系，应提供逻辑图。在有些场合可能还需要增加文字说明，描述功能要求。由于本例逻辑非常简单，P&ID 加叙述足够。

**D.3.2.6 选择失电关断或得电关断 (5.3.6)**

本 SIS 应失电关断。

**D.3.2.7 手动关断考虑 (5.3.7)**

将提供手动按钮和盘装报警，以便操作员可在 SIS 故障或观察到非正常状态时关断流量。

**D.3.2.8 SIS 失掉动力源时应采取的動作 (5.3.8)**

失电或失掉气源时，关断阀门。

**D.3.2.9 SIS 将过程处于安全状态的响应时间要求 (5.3.9)**



因罐进料缓慢，本 SIS 检测到液位高后动作的响应时间足够。

#### D.3.2.10 对显性故障的响应动作 (5.3.10)

如操作员知道 SIS 的任何故障，应立即按下紧急关断开关，关断所有进料。

#### D.3.2.11 人机界面要求 (5.3.11)

- a) BPCS 预报警；
- b) 手动关断能力；
- c) SIS 关断报警；
- d) SIS 诊断报警（见 D.4.2）。

#### D.3.2.12 复位功能 (5.3.12)

SIS 关断后，操作员要按下复位按钮，才能重新启动罐的进料。

### D.4 安全完整性要求 (5.4)

#### D.4.1 所需的 SIL (5.4.1)

需要 SIL 2。

#### D.4.2 诊断要求 (5.4.2)

关断阀上的限位开关将用来与逻辑控制器输出的阀门位置信号比较，如不相同，操作员将被告知有设备故障 [通过报警和（或）打印机]。

#### D.4.3 维护和试验 (5.4.3)

本 SIS 应每年检查和试验一次。此外，如检测到 SIS 任何故障，应立即进行纠正，且连续不停地工作，直至维修完毕。

#### D.4.4 谬误跳闸 (5.4.4)

谬误跳闸不会引起任何安全问题。

### D.5 概念设计 (6.0)

#### D.5.1 目的 (6.1)

下列各款定义了本 SIS 概念设计的要求。

##### D.5.1.1 考虑 (6.2.3)

- a) 分离：  
除共用的阀门外，SIS 应从 BPCS 分离。
- b) 冗余：  
需要冗余关断阀。
- c) 软件设计考虑：  
应用程序应使用功能块软件。
- d) 技术选择：  
本 SIS 可以使用任何认可的技术实现。本例选择 PES 以便对读者更有用。
- e) 故障率和故障模式：  
本设计中使用的 SIS 设备的故障率和故障模式已从 KIS2 公司收集的数据中得到。
- f) 结构要求：  
使用 KIS2 公司内部指南，SIL2 结构如下：

传 感 器	逻辑控制器	阀 门
1001	1001	2002

g) 动力源:

该批处理所需的电源、气源应使用好的工程惯例,应包括如下:

- 1) 专用动力源(参考 C.5, 250—5 和 250—26);
- 2) 动力源能够独立维护;
- 3) 动力源与非相关的动力源没有共模机械故障(主动力源集流排、集气管除外);
- 4) 接地系统采用好的工程惯例。

由于工厂电源系统可靠性高,不需要使用不间断电源。

h) 公共原因:

选择传感器和阀门减少化学药品粘附问题。

i) 诊断:

关断阀上的限位开关将用来与逻辑控制器输出的阀门位置信号比较,如不相同,操作员将被告知有设备故障[通过报警和(或)打印机]。

j) 现场设备:

所有过程测量应采用智能变送器。

k) 用户界面:

用户界面使用盘装的报警盘、手动复位开关和手动关断开关。

l) 安全:

KIS2 设施是安全的, SIS 逻辑控制器应放在控制室;

SIS 传感器和终端控制元件使用红色标牌(除标准标识外)将安全功能状态告诉给工厂人员;

所有智能变送器与 SIS 逻辑控制器的通信应有写保护,防止在线改变变送器的设定;

SIS 与 BPCS 的任何通信应有写保护,防止偶然从 BPCS 改变 SIS 程序。

m) 接线:

接线应遵循国家电气规程(参考 C.5)中的规范和规则以及 SIS 设备供应商指南;

设立两个独立的桥架系统,一个走电源(如 120V/240V),另一个走仪表信号(如 4mA~20mA);

SIS 可以与 BPCS 使用同一个接线箱,但所有 SIS 接线应使用不同的标识清楚的端子。

n) 文件:

符合 OSHA 29 CFR 1910 文件要求是必要的。

o) 功能试验间隔:

SIS 应每年试验一次。

## D.6 详细设计 (7.0)

### D.6.1 目的 (7.1)

下面是一个如何编制安全要求规格书的概述,以及如何使用 SIS 概念设计进行 SIS 详细设计。

### D.6.2 一般要求 (7.2)

KIS2 公司已编制了公司 SIS 详细设计指南。结构的选择采用 KIS2 公司指南和收集的资料。概念设计如图 D.2。

使用安全要求规格书、SIS 概念设计要求及 KIS2 公司内部指南可以进行 SIS 的设计。

使用这些文件,最终设计如图 D.2。

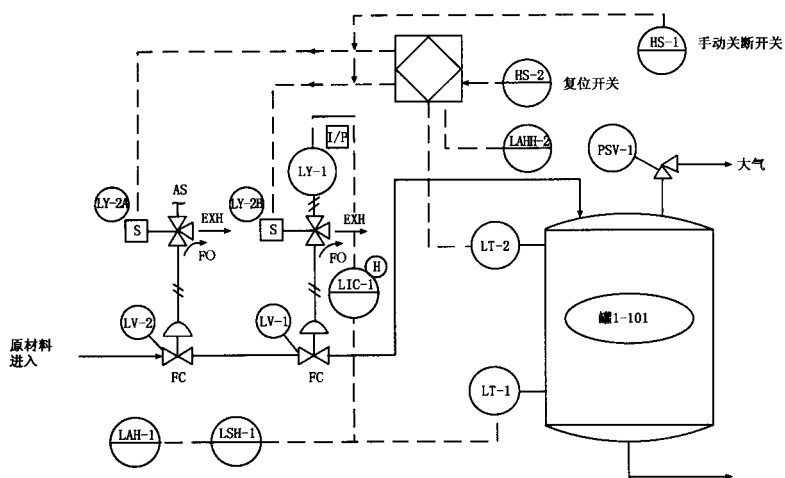


图 D.2 试验性设计方案