SHB

中国石油化工集团公司设计技术中心站标准

SHB－Z06－1999

石油化工紧急停车及安全联锁系统设计导则

Guide for the design of emergency shutdown and safety interlocking system for petrochemical industry

1999－10－12 发布　　2000－01－01 实施

中国石油化工集团公司自动控制设计技术中心站 发布

中华人民共和国行业标准
石油化工紧急停车及安全联锁系统
设计导则
SHB－Z06－1999

中国石化集团公司工程建设标准发行站出版发行

前　言

本导则是根据中石化(1996)建标字129号文，由中国石化集体北京石油化工工程公司负责编制。

在编制过程中，进行了广泛的调查研究，总结了多年来石油化工企业工程项目安全联锁设计的经验，征求了有关设计、建设、生产等方面的意见，吸取了美国、日本、欧洲等著名大型工程公司、行业协会和石油化工公司安全联锁系统设计的经验，对其中主要问题，进行了多次讨论，最后经审查定稿。

本导则在实施过程中，如发现需要修改或补充之处，请将意见和有关资料提供我公司，以便今后修订时参考。

我公司的地址：北京市亚运村安慧北里安园21号北京9721信箱
邮政编码：100101

本标准的主编单位：中国石油集体北京石油化工工程公司
主要起草人：顾祥柏　　黄步余

目　　次

1 总 则

1.0.1 为保障石油化工企业的安全生产，设置恰当的紧急停车及安全联锁系统，降低装置恶性事故发生的概率，减少计划外停车，避免重大人身伤害，重大设备损坏及重大经济损失的事故发生，特制定本导则。

1.0.2 本导则适用于石油化工装置（或工厂）紧急停车及安全联锁系统的工程设计，石油化工装置（或工厂）的辅助设施和公用工程的紧急停车及安全联锁系统工程设计也可参照执行。本导则不适用于液压与气动逻辑运算器。

1.0.3 紧急停车及安全联锁系统的设计，应遵循以下原则：

1 紧急停车及安全联锁系统原则上独立设置；

2 检测元件及执行机构原则上独立设置；

3 中间环节最少；

4 采用冗余或容错结构；

5 系统应是故障安全型。

1.0.4 执行本导则时，尚应符合国家现行有关标准规范的要求。

1.0.5 引用标准

1 Health and Safety Executive . Apr, 1991
Programmable Electronic Systems in Safety Related Applications

2 Instrument Society of America Committee. Feb, 1996, SP84.
Application of Safety Instrumented Systems for the Process Industries

3 IEC draft Publication 1508 · 1995.
Electrical/Electronic/Programmable Electronic Safety－Related Systems

4 石油化工企业仪表供电设计规定 SH 3082－1997

5 石油化工企业仪表供气设计规定 SH 3020－1997

6 石油化工企业仪表配管、配线设计规定 SH 3019－1997

7 石油化工企业仪表系统接地设计规定 SH 3081－1997

2 常用名词术语与缩写

2.1 常用名词术语

2.1.1 装置(Device)：由安全联锁系统监视、控制或保护的石油化工单元或机械设备。

2.1.2 危险(Hazard)：可引起人员伤害、设备破坏或环境污染等的潜在物理或化学条件。

2.1.3 冗余(Redundant)：有指定的独立的N:1重元件，并且可以自动地检测故障，切换到后备设备上。

2.1.4 冗余系统(Redundant System)：并行地使用多个系统部件，以提供错误检测和错误校正能力，该系统称为冗余系统。

2.1.5 容错(Fault Tolerant)：指有内部冗余的并行元件和集成逻辑，当硬件或软件部分故障时，能够识别故障并使故障旁路，继续正确执行指定功能的能力，或指硬件和软件发生故障，的情况下，系统仍然具有继续运行的能力。它往往包含三方面的功能：第一是约束故障，即限制过程或进程的动作，以防止错误在被检测出来之前继续扩大；第二是检测故障，即对信息和过程或进程动作进行动态检测；第三是故障恢复即更换或修正失效的部件。

2.1.6 容错系统(Fault Tolerant System)：具有容错结构的硬件与软件系统。

2.1.7 容错软件：能从故障状态恢复到正常工作状态的软件称为容错软件。故障恢复的方法可以用软件控制，也可用硬件控制。

2.1.8 容错技术：发现错误并纠正错误使系统继续正确运行的技术。包括错误检测和校正用的各种编码技术、冗余技术、系统恢复技术、指令复执、程序复算、备件切换、系统重新组合、检查程序、诊断程序等。

2.1.9 热后备(Hot backup)：有部分独立的N:1重元件和共用部件，可以自动或手动地检测故障，切换到后备设备上。

2.1.10 要求故障率(PFD：Probability of Failure on Demand)：安全联锁系统按要求执行指定功能的故障概率，是度量安全联锁系统按要求模式工作故障率的目标值。

2.1.11 安全度(SI：Safety Integrity)：安全联锁系统在一定条件、一定时间周期内执行指定安全功能的概率。

2.1.12 安全度等级(SIL：Safety Integrity Level)：安全联锁系统的安全等级，用PFD来定义。

2.1.13 可用度(A：Availability)：系统可使用工作时间的概率，用百分数计算：A＝MTBF/(MTBF＋MDT)。

2.1.14 可靠性(Reliability)：安全联锁系统在故障危险模式下，对随机硬件或软件故障的安全度。

2.1.15 紧急停车及安全联锁系统(ESD&SIS：Emergency Shurdown Safety Interlocking System)：用于监视装置(或独立单元)的操作，如果过程超出安全操作范围，可以使过程进入安全状态，确保装置(或独立单元)具有一定安全度的系统。

2.1.16 保护系统(Protected System)：专用于对装置中潜在的危险或不采取措施可能产生危险的事件发生响应，以减轻危险发生的后果或防止危险发生的系统。

2.1.17 故障安全(Fail－to－Safe(FTS))：故障时，使系统回到预定安全状态的能力。

2.1.18 显故障(Overt Fault)：是指能够显示故障自身存在的故障，是故障安全故障。

2.1.19 故障安全系统(Fail－safe System)：当控制回路中的输出元件或电路发生故障时，输出是非励磁的(或无效的)系统。

2.1.20 隐故障(Covert Fault)，是指不对危险产生报警，并允许危险发展的故障，是故障危险故障。

2.1.21 正常励磁模式(Normally Energized Mode)：在正常操作条件下，线圈是励磁的，在满足停车条件时线圈是非励磁的。

2.1.22 正常非励磁模式(Normally Deengerized Mode)：在正常操作条件下，线圈是非励磁的，在满足停车条件时线圈是励磁的。

2.1.23 系统故障(Systematic Fault)：由于系统设计或结构的错误以及环境条件引起的故障。

2.1.24 随机硬件故障(Random Hardware Failures)：由于硬件性能的下降而引起的故障。

2.1.25 可编程电子系统(PES：Programmable Electronics System)：基于微处理器的用于工厂控制、保护或监视，连接到检测元件和/或执行元件的系统。

2.1.26 硬件容错(HIFT：Hardware Implement Fault Tolerant)：利用专门设计的硬件电路实现诊断测试和故障隔离。

2.1.27 软件容错(SIFT：Software Implement Fault Tolerant)：用软件进行诊断测试和故障隔离。

2.1.28 共模故障(Common Cause Fault)：系统内或系统外可引起系统中多个元件故障的单个故障源。

2.1.29 诊断覆盖率(Diagnose Coverage)：可在线诊断出的故障占系统全部故障的百分数。

2.1.30 强制(Forcing)：可编程电子系统PES操作站跳过应用程序改变输入和输出状态的功能。

2.1.31 功能测试(Functional Testing)：周期性地检查ESD&SIS是否按照安全要求工作的测试。

2.1.32 一级安全度等级(SIL 1)：每年故障危险的平均概率为0.10～0.01即PFDavg＝0.10～0.01。

2.1.33 二级安全度等级(SIL 2)：每年故障危险的平均概率为0.01～0.001即PFDavg－0.01～0.001。

2.1.34 三级安全度等级(SIL 3)：每年故障危险的平均概率为0.001～0.0001即PFDavg－0.001～0.0001。

2.1.35 四级安全度等级(SIL 4)：每年故障危险的平均概率为0.0001～0.00001即PFDavg＝0.0001～0.00001。

2.2 缩写

PFD：要求故障概率(Probability of Failure on Demand)

PFS：故障安全概率(Probability of Failure in the Safe)

ESD：紧急停车(Emergency Shutdown)

PE：可编程电子(Programmable Electronic)

PES：可编程电子系统(Programmable Electronic System)

SIS：安全联锁系统(Safety Interlocking System)

TI：测试间隔(Test Interval)

MTBF：平均故障间隔时间(Mean Time Between Failures)

MTTF：故障前平均时间(Mean Time to Failure)

MDT：平均停车时间(Mean Downtime)

MTDF：平均故障诊断时间(Mean Time to Diagnose Fault)

MTTR：平均维修时间(Mean Time to Repair)

MTDL：平均故障定位时间(Mean Time to Determine a Fault Location)

MTTR：平均更换故障部件时间(Mean Time to Replace a Faulted Component)

MTRO：平均恢复操作条件时间(Mean Time to Return the Sysrem to Operable Condition)

PHA：过程危险分析(Process Hazard Analysis)

FCE：最终执行元件(Final Control Element)

PSAT：预开车验收测试(Pre－Start Acceptance Test)

MOC：修改管理(Management of Change)
EMI：电磁干扰(Electro Magnetic Interference)
RFI：无线电频率干扰(Radio Frequency Interference)

3 选用原则

3.1 独立设置原则

3.1.1 紧急停车及安全联锁系统应独立于过程控制系统，以降低控制功能和安全功能同时失效的概率，使ESD&SIS系统不依附于过程控制系统就能独立完成自动保护联锁的安全功能。

3.1.2 按需要配置相应的通讯接口，使过程控制系统能够监视ESD&SIS的运行状态。

3.1.3 原则上要求独立设置的部分有：

1 检测元件

2 执行元件

3 逻辑运算器

4 ESD/SIS与过程控制系统之间或其它设备的通讯

3.1.4 复杂装置的ESD/SIS宜合理地分解为若干子系统，各子系统宜相对独立。各子系统宜分组设置后备手动功能。

3.1.5 对不可能将ESD/SIS与过程控制系统分开的特殊情况(如气体透平控制系统包括控制和安全功能)，将控制和安全功能结合在同一系统中应考虑下面的因素：

1 确定公用元件和软件的故障及它们对ESD&SIS性能的影响。

2 在ESD/SIS与过程控制系统之间设置独立的分组后备手动功能。

3 确保ESD/SIS作用优先于过程控制的作用。

4 建立并保存ESD/SIS整个系统完整的修改、维护及测试文件。

3.2 选择采用技术的原则

3.2.1 ESD/SIS可采用电气、电子或可编程电子(E/E/PE)技术，也可以采用由它们组合的混合技术方案。

3.2.2 继电器的选用应满足下列要求：

1 继电器本质上不是故障安全的，继电器的触点可能粘在一起，也可能出现弹簧不能使开关触点返回非励磁位置。因此采用继电器逻辑系统应符合下面的原则：

a 确认继电器对安全应用是有效的；

b 继电器有好的"故障缓行"的位置特性；

c 放置继电器的环境是适当的(如完全密封)；

d 触点在线圈非励磁或故障时打开；

e 线圈带重力脱扣或双弹簧；

f 触点用适当的材料和等级；

g 安装限能负载电阻以防止触点粘接闭合；

h 提供适当的触点感应负载干扰消除器；

i 对低能量负载(如50伏或更低；10mA或更低)要求采用特殊的接点材料或设计(如密封触点)，消除触点氧化(如负载下降)引起操作的不可靠性的触点。当用这些特殊触点时，必须确定触点的故障模式，以确保构成故障安全的继电器系统。

2 下列情况不可用继电器：

a 高负荷周期性频繁改变状态；

b 定时器或锁定功能；

c 复杂的逻辑应用。

3.2.3 固态继电器

固态继电器适用于高负荷的应用，选用时应恰当处理好非故障安全模式。

3.2.4 固态逻辑

固态逻辑是将内部各种逻辑元件(如 AND, OR, NOT)用点接接线技术连接获得的逻辑功能。一般这些系统在故障安全要求方面(如不确定的故障模式)是受限制的。对 ESD&SIS 的应用一般不推荐固态逻辑。当固态逻辑系统用于 ESD&SIS 时，通常应采用 PES 作为诊断测试工具。

3.2.5 PES

PES 是指可编程序控制器、分散控制系统控制器或专用的独立微处理器，对下列情况，宜采用 PES 技术：

1 有大量的输入/输出，或许多模拟信号；

2 逻辑要求是复杂的，或包括计算功能的逻辑；

3 要求外部数据与过程控制系统进行通讯；

4 对不同的操作有不同的设定(跳车)点(例如批量控制，配方选择)。

3.3 结构选用原则

3.3.1 冗余结构既适用于软件又适用于硬件。

3.3.2 不宜采用可靠性较低的元件构成冗余，以防降低系统的可靠性。

3.3.3 冗余结构可采用但不限于下面的方法：

1 在知道参数间有一定的关系情况下，可以使用不同的测量方法(如压力和温度)；

2 对同一变量采用不同的测量技术(如质量流量计和涡街流量计)；

3 对冗余结构的每一个通道采用不同类型的可编程电子系统(PES)；

4 采用不同的地址(如冗余通讯介质的双路径)。

3.3.4 对存在共模故障(如仪表导压管的堵塞、腐蚀、电源故障等)的情况，宜采用不同技术的冗余结构。

3.3.5 选用 ESD/SIS 结构时，应确认下面的内容：

1 选择励磁停车或非励磁停车设计；

2 选择同类或不同类的冗余 ESD/SIS 检测元件，逻辑运算器和最终控制元件；

3 选择冗余的能源和 ESD/SIS 电源；

4 选择操作员接口部件(例如 CRT、报警指示灯、按钮)及它们连接到 ESD/SIS 的方法；

5 选择 ESD/SIS 与其它子系统(如 DCS)的通信接口和它们的通信方式(如只读或读/写)；

6 系统元件的故障率；

7 诊断覆盖率；

8 测试间隔。

3.4 故障安全型原则

3.4.1 ESD/SIS 应是故障安全型的。

3.4.2 ESD/SIS 的检测元件及最终执行元件在系统正常时应是励磁的，在系统不正常时应是非励磁的(即非励磁停车设计)。

3.5 中间环节最少原则

3.5.1 ESD/SIS 的中间环节应是最少的。

4 紧急停车及安全联锁系统工程设计的内容

4.1 可行性研究阶段

4.1.1 根据工艺装置的安全及自动化水平的要求，选择确定采用的安全联锁系统的方案，即选用继电器、固态逻辑电路或可编程电子系统。

4.1.2 与工艺设计人员共同讨论确定安全联锁系统的级别要求及涉及安全要求的 I/O 点数。

4.1.3 根据工艺要求的必要性及可行性确定采用何种类型的系统。

4.1.4 选择每个 ESD/SIS 安全功能采用的结构，以满足工艺过程的安全要求。

4.1.5 共模故障

当多个 ESD/SIS 功能组合到一个系统中时(共用逻辑或元件)潜在的共模故障将增多，应考虑编程、维护、电源、气源、保护等共模故障。

4.1.6 安全功能要求

多个安全功能共用元件应满足在系统中最严格的安全功能要求，非共用的系统元件必须满足与它们有关的安全功能的要求。

4.1.7 编制说明书。

4.2 基础工程设计阶段

4.2.1 根据可行性研究阶段确定的 ESD/SIS 的方案开展本阶段的工作(如果本开展可行性研究工作可与本阶段工作合并进行，并应符合 4.1 的要求)。

4.2.2 以管道仪表流程图(PID)及工艺安全联锁说明为依据，确定 ESD/SIS 的输入、输出信号种类、数量及与安全相关的其它逻辑的问题。

4.2.3 结合工艺装置的特点及控制要求，确定 ESD/SIS 所要实现的功能。

4.2.4 确定硬件的基本配置，画出初步的系统硬件配置图，主要内容应包括：

1 操作员接口(包括显示器，含灯、按钮、指示器和开关的盘，报警器，打印机，任何这些设备的组合)；

2 第一事故报警打印机；

3 与 DCS 的接口；

4 关的 I/O 点数。

4.2.5 考虑下列内容

1 独立配置的内容；

2 采用何种冗余措施；

3 选择采用的技术；

4 选择采用的结构；

5 故障率与故障模式的确定；

6 电源及气源系统的可靠性要求；

7 确定共模故障源；

8 是否采用诊断技术；

9 现场设备的选择与配置；

10 保护技术；

11 接线方法；

12 建立文档的内容；

13 功能测试间隔要求。

4.2.6 编制 ESD/SIS 系统规格书。

4.3 详细工程设计阶段

4.3.1 参照 ESD/SIS 规格书编制大纲的要求，根据基础过程设计确定的紧急停车及安全联锁的方案开展本阶段的工作，编制紧急停车及安全联锁系统规格书，发出正式的询价书，一般至少向三个 ESD/SIS 的供方询价。

4.3.2 ESD/SIS 供方的报价书至少要包括下面内容：

1 报价说明；

2 硬件配置清单及其功能说明；

3 可靠性数据(包括 MTBE、MTTR 等数据及计算方法)；

4 可靠性技术结构及其相应的安全论证的等级和证书；

5 对询价书中的安全要求的实现方法(软、硬件)；

6 系统硬件的分项价格；

7 应用软件由用户组态的分类价格；

8 产品的投运业绩。

4.3.3 ESD/SIS 系统报价书的评审，应包括以下内容：

1 ESD/SIS 的各种功能是否满足询价书的安全功能要求；

2 ESD/SIS 的硬件配置数量是否符合询价书的要求；

3 ESD/SIS 的安全质量指标(可靠性、MTBF、MTTR 等)是否先进；

4 硬件配置是否满足询价的冗余或二重化的要求；

5 软件是否标准化、模块化，是否经过实践；

6 价格比较。

4.3.4 配合采购部门进行 ESD/SIS 系统的合同谈判，合同技术附件可按照 ESD/SIS 技术规格书的要求进行，并清楚地讨论以下几个问题：

1 供货范围；

2 ESD/SIS 系统的软件组态谁负责；

3 修订的 ESD/SIS 系统规格书可作为合同附件之一。

4.3.5 与最终用户共同确定 ESD/SIS 系统选型及供货方，参加签定 ESD/SIS 系统供货合同、硬件清单、软件清单、备品备件及易损材料清单、初步的进度表。

4.3.6 合同签定后4～6周，可召开设计条件会议。由供货方向用户提供控制室 ESD/SIS 系统的安装、供电、接地、空调等设计条件，并列出双方资料交付的时间表。

4.3.7 准备组态所需的基础数据、图纸等设计文件：数据表，逻辑图或说明，逻辑监控画面，第一书故报警打印要求，报表，重要工艺数据的存储要求。

4.4 ESD 及安全联锁应用软件组态、生成阶段

4.4.1 供方组态

1 向供方提交应用软件组态所需的设计文件，参加有关工程会议，向供方作设计交底；

2 检查供方的系统配置、应用软件组态、生成的结果是否满足设计要求。

4.4.2 用户与供方合作组态方式，组态的具体工作由用户完成，供方负责组态文件审查和生成指导及结果确认工作。

4.4.3 组态生成。

4.5 安装、调试、投运阶段

4.5.1 设计人员参加配合安装调试及投运工作。

5 硬件配置

5.1 配置原则

5.1.1 根据 ESD/SIS 的规模及功能需求以及工序与管理的划分等因素考虑有关的硬件配置。

5.1.2 复杂装置和重要机组的 ESD/SIS 应独立于过程控制系统。

5.1.3 ESD/SIS 不依附于过程控制系统就能独立完成自动保护联锁功能。

5.1.4 复杂装置的 ESD/SIS 可合理地分解为若干子系统，各子系统宜相对独立。

5.1.5 过程控制系统可监视 ESD 及 SIS 的运行状态(按需要配置相应的接口)。

5.1.6 所选硬件应满足安全级别要求，并参照下列原则选用：

1 小于 40 个输入输出点不含运算功能的 ESD/SIS，宜选用继电器系统；

2 大于 40 个小于 100 个输入输出点不含运算功能的 ESD/SIS，宜选用固态继电器系统；

3 大于 40 个小于 100 个输入输出点含运算功能的 ESD/SIS，宜选用小型可编程电子系统；

4 大于 100 个输入输出点的 ESD/SIS，宜选用可编程电子系统。

5.2 用户接口

5.2.1 操作员接口

操作员接口用于操作员和 ESD/SIS 之间的信息通讯(包括：显示器，含灯、按钮、指示器和开关的盘，报警器，打印机，任何这些设备的组合)。

1 显示器

a 显示器可同时有安全和过程控制功能。过程控制系统或其它的计算机控制系统，通过正常的操作员显示，为 ESD/SIS 提供唯一的操作员接口。

b 在紧急条件下，操作员和 ESD/SIS 之间数据更新和刷新的通信速率应满足安全响应的要求。

c 对于有关 ESD/SIS 的显示应清楚地按避免使操作员在紧急状态下混淆的多义性或潜在性标识。

d 操作员应易于访问与安全有关的显示，尽可能有单个的键盘锁或触屏锁提供显示等级。

e 给操作员在一幅显示画面中有足够的信息，快速地传送关键信息，同时应提供用在非有关安全的显示相同的访问方法、常规报警和显示部件。

f ESD/SIS 的显示应注意下列问题：

1) 用颜色、闪亮指示器和适宜的数据显示指导操作的重要信息；

2) 减少混淆的可能性；

3) 信息必须是清楚的、不易混乱的。

g 操作员接口和相关的系统(如 DCS)可以用于提供自动的安全有关的事件记录和报警功能。记录的条件应包括 ESD/SIS 事件(例如停车和出现预停车)及无论什么时候 ESD/SIS 的程序修改和诊断的记录。

2 盘

1 盘应置于操作员易于操作的地方；

2 盘布置应确保按钮、灯、表头或其它元器件的布置不使操作者混淆；

3 应在物理上分开不同工艺单元的易引起误操作的停车开关及外形相似的设备，并用标签标

上它们的功能；

4 提供测试所有灯的方法。

3 打印机

a 打印机联接到 ESD/SIS，并且如果打印机故障、切断电源、断线、没有纸或非正常，应不影响安全功能；

b 如果 ESD/SIS 接到过程控制系统，则可以使用过程控制系统装备执行安全有关的记录和报表功能；

c 打印机通常对形成事件顺序(SOE)信息、诊断和其它的安全有关的事件和报警；

d 如果打印是一个缓冲功能(存储信息按要求或按时间表打印)，缓冲区应规定大小以便不失去信息。

5.2.2 维护/工程接口

1 维护/工程接口可对 ESD/SIS 进行编程、测试和维护，并应具备以下功能：

a 系统硬件组态；

b 应用软件开发，文件下装到 ESD/SIS 逻辑计算器；

c 为修改、测试和监视访问应用软件；

d 查看 ESD/SIS 系统资源和诊断信息；

e 修改 ESD/SIS 安全等级和访问应用软件变量。

2 维护/工程接口应有能力显示所有 ESD/SIS 元件的操作和诊断状态(如输入/输出模件、处理器等)包括在他们之间的通讯。

3 维护/工程接口应提供拷贝应用程序的存贮介质。

5.3 过程接口

5.3.1 类型的选择

各类 I/O 卡件的品种必须与现场信号源或负载匹配。

5.3.2 过程接口的关联设备

1 隔离器：在输入/输出接口前宜设置隔离器；

2 安全栅：凡信号来自或送至爆炸危险区域，按照防爆要求采用本安防爆等级时，在输入/输出接口的现场侧加隔离型安全栅；

3 旁路维护开关：根据工艺要求对输出加并联旁路维护开关；

4 继电器：数字量输出宜采用继电器进行隔离。

5.3.3 过程接口的冗余

过程接口应按照 ESD/SIS 系统规格书的要求配置相应的冗余结构。

5.3.4 过程接口的备用

1 备用点不宜超过 10%；

2 卡件空槽位为 10…15%。

5.4 逻辑运算器

5.4.1 逻辑运算器应按照安全规格书配置相应的安全结构(如冗余或容错结构)。

5.4.2 逻辑运算器 CPU 的负荷不得超过 80%。

5.4.3 逻辑运算器的平均故障间隔时间(MTBF)、隐故障模式、可识别的隐故障出现的频率应满足工艺要求。

5.4.4 逻辑运算器应带防止隐故障的方法(内部的或外部的，如过程动作的逻辑运算器性能的比较、用应用软件测试逻辑运算器的性能等)。

5.4.5 除非工艺过程允许自动重新启动，一般逻辑运算器应确保在恢复通电时不自动重新启动。

5.5 通讯接口

5.5.1 通讯接口与总线应采用冗余配置。

5.5.2 通讯总线应符合国际标准。

5.5.3 通讯距离应能满足装置的实际要求。

5.5.4 通讯总线的负荷不应超过60%。

5.5.5 有与DCS或管理计算机的通讯接口。

5.5.6 有连接通用共用网络(如工厂管理网)的接口，可进行必要的网间数据传输。

5.5.7 通讯接口故障不影响ESD/SIS使过程进入安全状态的能力。

5.5.8 采用屏蔽电缆或光纤等将通讯信号与其它能源隔离开。

5.6 电 源

5.6.1 系统内部电源应是带电池后备的冗余电源。

5.6.2 外部负载电源应是独立的(UPS电源)。

6 现场设备

6.1 检测元件

6.1.1 ESD/SIS的检测元件宜独立设置。

6.1.2 ESD/SIS的检测元件不依赖于过程控制系统。

1 DI转接：先进ESD/SIS再进过程控制系统；

2 DI并接：经继电器隔离后分别进ESD/SIS和过程控制系统；

3 AI：4－20mADC先转换成1－5VDC后分别进ESD/SIS和过程控制系统；

4 RTD：先经ESD及SIS的AI－RTD卡，再经相关的通讯接口进入过程控制系统。RTD经温变转换成4－20mADC信号，再转换成1－5VDC后分别进ESD/SIS和过程控制系统。

5 选择热电偶、热电阻断线时ESD/SIS的功能应能实现只报警，而不误动作。

6.1.3 以下关键部位的检测元件宜3取2配置或2取2配置：

1 大型机组的润滑油压力低低联锁；

2 大型机组的超速开关；

3 乙烯裂解炉进料量；

4 裂解气压缩机轴位移、吸入罐液位；

5 乙烯装置分离塔的压力；

6 加氢循环氢离心压缩机的入口分离器液位高高开关；

7 加氢高压分离器液位低低开关；

8 催化裂化主风低低流量开关。

6.1.4 关键部位的温度、压力、液位、流量开关宜采用电子式。

6.1.5 采用智能检测元件时，应采取一定的保护措施(如禁止从操作台修改现场仪表的有关参数)。

6.1.6 检测元件的冗余可选用两个模拟元件，两个开关检测元件(开关)，或者一个模拟元件一个开关检测元件。选用两个模拟设备可提供可用性更好的保护。

6.1.7 模拟设备优先于开关型的设备。

6.1.8 尽可能采用冗余或不同的元件测量可显示相同不正常条件的不同变量。

6.1.9 仔细地检查能够影响导压管满管和空管的过程/环境条件。

6.1.10 对膜片密封，检查密封液以防止混合、冻结、聚合等所有能够引起错误读数的情况。

6.1.11 选择满足系统可靠性要求并有足够好可靠性的不同设备或者考虑可用的两种不同的方法。

6.1.12 对ESD/SIS的应用，在工艺过程和元件之间应按所用的切断阀最少。

6.1.13 每一个要求工艺侧切断的元件应有自己指定的取源口和阀门。

6.1.14 避免超出元件精度极限的测量(如当检测零流量时，将不采用流量元件)。

6.2 执行元件

6.2.1 ESD/SIS的输出原则上应有独立的执行器，当工艺条件允许与正常控制共用执行器时，可采用由ESD取代切换方式执行ESD的事故命令。

6.2.2 ESD/SIS输出与电控动力设备之间宜采用继电器隔离。

6.2.3 采用智能定位器时，应采取相应的保护措施。

6.2.4 电磁阀的选用，应符合下列要求：

1 应选用长期带电，低功耗的电磁阀；

2 考虑温度、压力、防爆区域划分、负载等；

3 对阀门的最小、最大供气压力的影响；

4 确保电磁阀的尺寸是恰当的；

5 不宜带现场手动复位；

6 采取防止电磁阀放空端堵塞、脏、冻结等措施。

6.2.5 与安全有关的控制阀不应设置现场手动的功能(应带安全复位功能)。

6.2.6 当执行元件故障时，应有报警反馈，并进入到维护状态。

6.2.7 执行元件以下特性应满足 ESD/SIS 的安全要求。

1 打开/关闭速度；

2 在流向的两个方向的切断差压；

3 泄漏等级(要求切断密封的程度)；

4 本体和执行器防火等级；

5 在同一位置长期的性能。

6.2.8 在满足要求的地方，尽可能考虑使用调节阀作为最终执行元件，以便通过检查阀门是否停留在同一个位置上诊断控制回路是否正常。

6.2.9 考虑故障位置与流向开关位置。

6.2.10 最终元件宜带阀位指示。

6.3 现场设备选用注意事项

6.3.1 与安全有关的检测元件与执行元件不宜直接挂在现场总线上，当现场设备由非 ESD/SIS 命令改变状态时，应引起报警。

7 软件编制

7.1 软件编制原则

7.1.1 编程语言应是成熟的或是经按工业标准验证可以接受的。

7.1.2 编制应用软件所用的工具软件应满足下面的条件：

1 供应商有软件质量计划；

2 工具软件版本应是成熟的；

3 工具软件版本应完全适用于所选用的 ESD 及 SIS 的硬件环境；

4 在更新工具软件的版本时，应确认其增强的、固化的软件功能的可靠性及与旧版本的兼容性，在原有应用软件的性能确保能得到保证与提高后，可更新工具软件的版本，并完善更新相应的文档。

7.1.3 应用软件包的使用除应具备本规范第7.1.2条的条件外，应用软件应用于 ESD/SIS 的用户程序开发时，需要进行必要的测试，并得到 ESD/SIS 设备制造厂的推荐确认后，方可使用。

7.1.4 ESD/SIS 的应用软件应采用模块设计。

7.1.5 模块设计应强化设计的简单性及集成度。

7.1.6 禁止使用直接转向语句。

7.1.7 为了避免程序不必要的复杂性和系统难于预测的运行特点，软件编制应考虑下面的因素：

1 软件应有一个确定的顺序和结构，以确保用户在 ESD 及 SIS 软件工作的整个过程内了解应用程序；

2 如果采用顺序程序块，应尽可能将块压缩在最少的层中；

3 应用程序应进行必要的审查与比较后方可投入正式应用。

7.2 软件编制的安全性要求

7.2.1 为防止维护人员和操作人员修改程序，应该在 ESD 及 SIS 中安装一些锁定程序修改的设备。

7.2.2 ESD 及 SIS 的应用软件应由授权的专业人员管理与维护。

7.2.3 采用 PROM 或 EPROM 存储器存储程序，并应提供有效防止非被授权人员修改程序的功能。

7.2.4 应用软件宜采用包括验证等的诊断测试方案，以确保应用软件的安全性。

7.2.5 编程时宜采用非保持输出。

7.2.6 如果输出必须锁定，则应采用一个保持电路。

7.2.7 ESD/SIS 程序中为测试系统和检查系统而设置的强制 I/O，在系统投入正常使用时，应将强制 I/O 的功能取消。

7.3 软件审查

7.3.1 ESD/SIS 的程序应与逻辑框图一致。

7.3.2 分析证实在 ESD/SIS 规格书中的每一个要求已在软件设计中实现。

7.3.3 审查比较安全关键功能的设计。

7.3.4 用键盘输入那些正常边界以外的数据和其它动作的实例对软件进行测试。

7.3.5 检查 ESD 及 SIS 应用软件的实现缺陷报告和消除缺陷系统。

7.3.6 测试应用软件，确定软件对存在的硬件故障发生作用的情况。

7.4 软件工程文件

7.4.1 软件源程序清单。

7.4.2 软件的程序框图。

7.4.3 软件采用的主要参数及变量。

7.4.4 逻辑框图及说明。

7.4.5 软件版本、程序说明、用户手册、使用说明等软件标准文档。

8 配线及接地工程要求

8.1 配线工程要求

8.1.1 接线应满足制造商的推荐和有关设计规范的要求。

8.1.2 对 ESD/SIS 的接线宜采用下面的措施：

1 ESD/SIS 与现场设备的通道应是独立的电路；

2 采用隔离电路，避免电感和电容耦合使输入误通；

3 实现测试能力；

4 加保险丝隔离故障以减少共模故障；

5 将 ESD/SIS 的端子与所有其它的端子分开。

8.1.3 对电子或可编程电子 ESD/SIS 的接线，应满足下列的要求：

1 采用总屏对屏双绞线信号电缆以抗电磁干扰(EMI)；

2 在电源末端用屏蔽和泄放线接地以抗无线电频率干扰(RFI)；

3 所有的金属覆盖(如电缆铠层)或敷设通道(如电缆槽板、穿线管)对电干扰(EMI)和防雷保护应在一端接地，也可根据距离的长短设中间接地点；

4 将不同的能量级分开，取消交叉干扰和电磁噪声；

5 采用恰当的浪涌保护；

6 提供在不同的接地级别间的隔离(如光纤)；

7 数据通信电缆规格和屏蔽应满足制造厂的推荐；

8 机柜接线应减少电气噪声干扰和避免产生高温。

8.1.4 非屏蔽的控制柜内不宜用低电平逻辑。

8.1.5 采用固态输入或输出时，应注意避免泄漏电流使执行元件误动作。

8.2 接地工程要求

8.2.1 ESD/SIS 应用中，应解决电浮地问题(如在 UPS 后加隔离变压器时)。

8.2.2 接地电阻应满足 ESD 及 SIS 设备制造厂商的推荐要求，采用与制造厂推荐不一致的接地方法应有制造厂的确认。

8.2.3 从电气到电子到可编程电子设备时，接地的限制变得越来越严格。因此，电气设备可以接到为电子或可编程电子设备设计的接地系统中。电子设备接地可以接到为可编程电子设备设计的接地系统中。不允许可编程电子设备接到为电气技术而设计的接地系统。

8.2.4 接地系统应确保是单点接地。

8.2.5 接地端子及接地体应采用防腐蚀保护措施。

8.2.6 接地体安装完成应进行有关的测试。

8.2.7 安全联锁系统的安全接地应与防雷接地系统进行隔离。

8.2.8 屏蔽层应接地。

8.2.9 采用电气、电子可编程电子技术的复合系统，如果制造厂未提供专用的安装方法，应按照可编程电子接地考虑接地系统。

9 安装、调试、预开车验收

9.1 安装

9.1.1 设备安装应符合设计及制造厂要求。

9.2 调试

9.2.1 调试应确保 ESD 及 SIS 按照详细设计的要求进行安装，并具备预开车验收测试条件。

9.2.2 调试应包括但不限于下面的内容：

1 设备安装与接线是正确的；

2 提供的电源与气源满足要求并具备使用条件；

3 所有仪表已调校；

4 现场设备具备使用条件；

5 逻辑运算器与输入/输出设备运转正常。

9.3 预开车验收测试(PSAT)

9.3.1 PSAT 提供满足 ESD/SIS 系统规格书的所有 ESD/SIS 功能测试。PSAT 期间应确认包括但不限于下列内容：

1 SIS 与过程控制系统或任何其它系统或网络的通讯；

2 按照安全要求规格书检查检测元件、逻辑计算和最终执行元件；

3 按照安全要求规格书确定安全设备的设定点及动作；

4 激活专用的停车顺序；

5 ESD 及 SIS 提供专用的报警和操作显示画面；

6 计算精度满足 ESD 及 SIS 的要求；

7 系统的全部或部分复位功能；

8 旁路与旁路复位功能操作的正确性；

9 手动停车系统操作的正确性；

10 维护程序的测试间隔与安全要求一致；

11 SIS 文件与实际安装和操作程序一致。

9.3.2 用于 PSAT 测试仪表的精度与实际应用仪表的精度一致。

9.3.3 ESD/SIS 操作规程应在调试与预开车验收测试期间完成，文件至少应包括下列内容：

1 测试过的 ESD/SIS 标志；

2 调试完成的确认签署；

3 执行 PSAT 的日期；

4 用于 PSAT 的参考步骤；

5 PSAT 满足要求的签署。

附录 A 紧急停车及安全联锁系统规格书编制大纲

A.1 主要内容

A.1.1 安全要求规格书的主要内容应包括但不限于下列的内容：

1 列出安全功能要求清单；

2 每一个安全功能的安全度；

3 与 ESD/SIS 相关的控制要求；

4 工艺过程(如腐蚀、堵塞等)可引起的过程共模故障；

5 与 ESD/SIS 相关的每一个危险事件所涉及到的最终执行元件、事件起源、动态响应等过程信息；

6 与安全要求相关的 I/O 清单。

A.2 功能要求

A.2.1 安全功能要求主要包括但不限于下列的内容：

1 对每一个指定的事件定义过程的安全状态；

2 ESD/SIS 的过程输入和它们的设定点；

3 过程变量的正常操作范围与操作极限；

4 ESD/SIS 的过程输出及其动作；

5 过程输入和输出的功能(如逻辑运算功能等)关系；

6 励磁或非励磁停车；

7 手动、自动停车；

8 ESD/SIS 失去电源气源后的动作；

9 ESD/SIS 响应时间要求；

10 故障安全故障的响应动作；

11 复位功能；

12 旁路/强制输入/输出要求。

A.3 系统要求

A.3.1 系统要求，应包括以下内容：

1 人机接口要求；

2 安全系统结构图；

3 安全系统通信要求；

4 电源及气源要求；

5 安全系统输入/输出要求；

6 开发程序工作站及软件要求；

7 备用容量要求(内存、I/O 等)。

A.4 安全要求

A.4.1 安全要求应包括以下内容：

1 每个安全功能的安全要求；
2 获得安全要求的诊断要求；
3 获得安全要求的维护及测试要求；
4 对危险的误停车可靠性的要求。

A.5 文件、服务及其它

A.5.1 文件、服务及其它：
1 检查与测试要求；
2 安全系统文件；
3 安装及预开车验收要求；
4 培训；
5 备品备件；
6 保证。

附录 B 操作维护

B.1 操作

B.1.1 ESD/SIS 的操作维护人员应在操作前进行培训。

B.1.2 用户有相应的操作文件并保证是最新版本。

B.1.3 ESD/SIS 操作步骤程序应包括 SIS 正确的安全操作方法说明。这些操作程序一般是按单元操作程序编写，这些程序应包括但不限于以下内容：
1 安全操作极限（如跳车）和超出极限的安全含义；
2 ESD/SIS 如何使过程进入安全状态；
3 旁路系统复位、操作权限等的正确操作方法；
4 ESD/SIS 报警与跳车的正确响应。

B.2 维护

B.2.1 建立包括 ESD/SIS 维护、测试和维修的写保护维护规程。

B.2.2 ESD/SIS 维护应包括但不限于下列内容：
1 ESD/SIS 的定期功能测试；
2 检测到的故障维修及维修后的相应测试；
3 定期常规维护（如更换润滑油、通风过滤器、电池和按钮等）。

B.3 测试、检测与维修

B.3.1 制造厂的 SIS 维修和测试要求手册应包括维修规程。

B.3.2 用户有周期性检测 SIS 设备故障和损坏等的检查程序。

B.3.3 对进行旁路测试、检查和维修时过程是危险的情况，应有严格的保护过程安全的管理规程。

B.4 功能测试

B.4.1 按照指定的程序进行周期性的功能测试，以防止隐故障影响 ESD/SIS 执行安全功能。

B.4.2 功能测试包括检测元件、逻辑运算器和最终执行元件的整个 ESD/SIS 系统。

B.4.3 功能测试的频率

1 ESD/SIS 应按照安全要求规格书确定的频率计算出相应的测试间隔，ESD/SIS 的不同部分可以有不同的测试间隔；

2 测试间隔可由用户根据历史操作经验、软件与硬件的可靠性等因素进行适当的调整；

3 任何应用逻辑的修改，都应进行全面的功能测试，除非部分测试能够确保 ESD/SIS 系统的安全要求。

B.4.4 功能测试步骤

1 对每个 ESD/SIS 应提供说明功能测试每一步骤应如何执行的文件。

2 在功能测试期间检测出的缺陷应在确保安全的条件下或停车时进行修复。

3 功能测试应检查包括不限于下列内容：

a 包括检测元件、ESD/SIS 输入模件的所有输入设备的运行状态；

b 每个输入设备相关的逻辑；

c 所有输入的跳车设定值；
d 报警功能；
e ESD/SIS 的响应速度；
f 逻辑操作顺序；
g 全部最终执行元件和 ESD/SIS 输出模件的功能；
h ESD/SIS 执行的计算功能；
i 手动跳车功能；
j 用户诊断功能；
k ESD/SIS 系统的全部功能；
l 测试后，将 ESD/SIS 切回正常使用状态。

B.4.5 在线功能测试

1 对于没有测试经验的执行元件，在装置停车期间应对执行元件进行功能测试。在线测试期间对测试的输出应有足够的经验(如输出继电器、切断电磁阀、部分阀门的动作等)。

2 应明确允许进行在线功能测试的步骤。

B.5 功能测试文件

B.5.1 用户应保存已执行的测试与检测的记录。

B.5.2 功能测试文件至少应包括下面的内容：

1 检查日期；
2 设备的系列号或回路号、位号、设备号等唯一的标识；
3 执行测试或检查人员的名单；
4 检查测试的结果("发现的"与"遗留的"问题)。

附录 C 修改管理

C.1 修改管理规定

C.1.1 对下面内容的修改应明确修改步骤：

1 操作步骤的修改；
2 新的或修改的安全法规引起的必要的修改；
3 工艺过程要求的修改；
4 安全要求规格书的修改；
5 软件与硬件错误的修改；
6 系统故障的修改；
7 应用软件的修改；
8 降低故障率的修改。

C.1.2 MOC 规定应考虑下面的因素：

1 修改的技术基础；
2 修改对安全与健康的影响；
3 操作方法的修改；
4 修改所必需的修改时间；
5 可用内存空间；
6 有效响应时间；
7 修改要求的授权签署。

C.1.3 修改审查应确保满足下面的要求：

1 保持原来的安全等级要求；
2 修改审查的人员应具备审查的资格。

C.1.4 在装置开车前或修改实施前应将修改内容通知有关的人员，并对其进行培训。

C.2 修改管理文件

C.2.1 在开车前，所有的操作方法、过程安全信息和 ESD 及 SIS 文件(包括软件)应进行更新与修改。

C.2.2 应防止对文件的非权威的修改、损失或丢失。

C.2.3 所有文件应按照一定的程序进行更新版本、审查、修改与确认的管理。

附录 D　ESD/SIS 系统详细设计工作内容摘要

D.1　一般要求

D.1.1　确定每个安全功能的安全度。

D.1.2　满足 SIL 要求的 ESD/SIS 的设计。

D.1.3　包括使过程保持在安全状态的顺序功能的设计。

D.1.4　包括一个或多个安全联锁功能 SIS 的设计。

D.1.5　确定 ESD/SIS 的设计文件的版本及版本升级管理规程。

D.1.6　ESD/SIS 设备制造商应保持包括设备应用软件等的正式版本及升版程序，并用可见的标记或用户接口标识版本的信息，如部件号(PART NO)、系列号(Serial No)、批量号(Batch No)。

D.1.7　确保采用的软件与硬件是恰当的。

D.1.8　任何由 ESD 及 SIS 实现的非安全功能的动作，应不中断或影响 ESD/SIS 的任何功能。

D.1.9　确定安全功能的每一个 ESD/SIS 元件的安全状态。

D.1.10　过程进入安全状态，并保持在安全状态，直到复位的有关 ESD/SIS 设计。

D.1.11　对采用手动复位或自动复位进行定义。

D.1.12　提供独立于逻辑运算器直接操作 ESD/SIS 最终执行元件的功能的 ESD/SIS 设计。

D.1.13　满足环境与相应危险区等级的 ESD/SIS 设计要求。

D.1.14　ESD/SIS 输入/输出的供电回路的设计，通常与用于任何其它用途的供电回路分开，除非检测元件、最终执行元件与过程控制系统共用。

D.2　ESD/SIS 逻辑运算器

D.2.1　逻辑运算器供应商应提供包括输入模件、输出模件、维护接口设备、通信和应用软件的完整设计，并将其形成文件。

D.2.2　逻辑运算器供应商应提供平均故障时间(MTBF)的数据，隐故障模式清单，可识别的隐故障出现的频率及这些数据的来源和计算方法。

D.2.3　PES 逻辑运算器应提供防止隐故障的方法(内部的或外部的，如过程动作的逻辑运算器性能的比较、用应用软件测试逻辑运算器的性能等)。

D.2.4　逻辑运算器应与过程控制系统分开。对于不分开或分不开的 SIS 应用(如气体透平等)情况，逻辑运算器应能满足 ESD/SIS 的安全要求。

D.2.5　除非过程危险分析(PHA)表明允许自动重新启动，一般逻辑运算器应确保在恢复上电时不自动重新启动。

D.3　现场设备

D.3.1　一般要求

1　对励磁停作，数字输入/输出电路应采用终端监视等方法。

2　当用远方输入/输出时，应对逻辑运算器的连接性能进行评价。

3　除下列情况外，每个独立的现场设备应有指定的接到系统输入/输出的接线方式。

a　多个元件中接到一个输入；

b　连接到单个输出的最终执行元件；

c　用户确认的如火灾和气体检测报警系统；

d　现场总线。

4　选用和安装的现场设备应能够满足过程与环境条件，以防止包括腐蚀、介质冻结、悬浮固体颗粒、聚合结焦、温度与压力过限等条件引起测量不准确。

D.3.2　检测元件要求

1　除非经过安全审核确认可以读/写，一般 ESD/SIS 的智能元件应有写保护，以防止远方的不慎修改。

2　ESD/SIS 的元件应与过程控制的元件分开，但下列两种情况除外：

a　采用冗余元件，同时连接到过程控制系统和 ESD/SIS，并且当过程控制系统故障时，不影响 ESD/SIS 对元件的正常操作或读入；

b　如果过程危险分析确定过程控制系统需要一个或更多的保护，那么 ESD/SIS 应为过程控制系统提供元件冗余保护。

3　制造厂或用户提供的元件诊断应满足安全的要求。

D.3.3　执行元件要求

1　对 SIL3，单个的过程控制系统调节阀不能用作唯一的执行元件。对 SIL1 和 SIL2，采用单个过程控制系统调节阀作为最终元件，要进行安全检查。

2　电机启动器(如动设备、电动阀门等)一般既可以用于过程控制系统又可以用于 ESD/SIS，除非过程危险分析明确指出其他要求。

D.4　接　口

D.4.1　操作员接口(包括 CRT、指示灯、按钮、喇叭、报警系统等)，应满足下列要求：

1　SIS 的操作员接口是操作员将过程处理成安全状态的人机接口。操作员接口应满足 ESD 及 SIS 自动功能不完善时的操作要求。

2　操作员接口显示应包括但不限于 SIS 的下列内容：

a　ESD/SIS 的动作状态；

b　保护功能旁路；

c　选举功能退化(如 2003 到 1002)指示和出现故障的状态；

d　检测元件和最终执行元件的状态；

e　停电/停气指示；

f　各种诊断结果；

g　ESD/SIS 有关设备故障状态指示。

3　操作员接口禁止的操作：

a　禁止修改 ESD/SIS 应用软件；

b　禁止修改 ESD/SIS 操作程序；

c　如果 ESD/SIS 工程维护接口用作 ESD/SIS 的操作员接口，从该接口修改应用软件应有安全确认和修改保护；

d　允许有关安全信息由过程控制系统传到 ESD/SIS，对这类应用，仅限于过程控制系统可以访问的 ESD/SIS 变量，并应有确认程序，以确保传送到 ESD/SIS 的及 ESD/SIS 接受的内容是正确的；

e　操作员接口的读/写访问权通过维护工程接口进行组态或编程确定，并有相应的文件与保护方法。

D.4.2　工程维护接口，应符合下列要求：

1　工程维护接口要求

a 工程维护接口提供 ESD/SIS 的维护功能，包括软件指导与诊断、编程、诊断工具、状态指示、设备旁路、设备测试与设备校验；

b 工程维护接口故障不影响 ESD/SIS 的安全功能，也就是说在正常操作时，可以切断 ESD/SIS 的工程维护接口。

2 工程维护接口应提供下面的功能

a 对 ESD/SIS 的操作模式、编程、数据、测试、旁路、维护等提供访问保护；

b 调用 ESD/SIS 诊断功能和故障处理功能；

c 增加、删除、修改应用软件的功能；

d 调用 ESD/SIS 故障清单数据。

D.4.3 通信接口是指在 SIS 与操作员接口、维护工程师接口、过程控制系统、网络或外设等其他设备的软件与硬件通信设备，应满足下列的要求：

1 ESD/SIS 通信接口故障时，不应影响 ESD/SIS 使过程进入安全状态的能力；

2 通过采用屏蔽电缆或光纤等将通信信号与其它能源隔离开。

D.5 电源与气源

D.5.1 确定安全功能对每个电源与气源的要求，ESD/SIS 的电源与气源应满足安全功能的最高要求。

D.6 系统环境

D.6.1 应提供下列设置 ESD/SIS 的环境条件：温度、湿度、接地、污染（毒气、灰尘、油污等）、电磁干扰（EMI；Electro－Magnetic Interference）、无线电频率干扰（RFI；Radio Frequency Interference）、震动、静电、电气防爆区域等级、雨淋等。

D.6.2 所有的 ESD/SIS 元件应满足相应的环境要求。

D.6.3 对于不能满足环境要求的 ESD/SIS 设备应采取如安装加热系统、强制通风、空调、空气过滤器等措施。

D.7 应用逻辑要求

D.7.1 应提供用于 ESD/SIS 的应用逻辑的正式版本和升版文件。

D.7.2 用户应提供与保留应用软件的正式版本和升版管理方法。

D.7.3 用户应确保应用逻辑的文件是清楚的、准确的、完整的。

D.8 维护与测试设计要求

D.8.1 ESD/SIS 应能够对全系统进行测试。当计划的过程停车间隔比功能测试间隔大时，则要求 ESD/SIS 有在线测试能力。

D.8.2 当 ESD/SIS 有在线测试功能时，应同时具备在线测试 ESD/SIS 隐故障的能力。

D.8.3 当 ESD/SIS 具有测试或旁路功能时，应确认下列的内容：

1 ESD/SIS 的维护与测试应满足安全要求；

2 操作员可以按正常或报警操作程序使 ESD/SIS 旁路；

3 ESD/SIS 的旁路将不失去对所有监视条件的检测与报警。

D.8.4 下面部分不能采用强制输入/输出：

1 应用软件；

2 操作程序；

3 维护（除非有步骤并带保护的强制，并且对这些强制有报警）。

用词说明

对本导则条文中要求执行严格程度不同的用词，说明如下：

1 表示很严格，非这样做不可的用词

正面词采用“必须”；

反面词采用“严禁”。

2 表示严格，在正常情况下应这样做的用词

正面词采用“应”；

反面词采用“不应”或“不得”。

3 表示允许稍有选择，在条件许可时首先应这样做的用词

正面用词采用“宜”；

反面词采用“不宜”。

表示有选择，在一定条件下可以这样做，采用“可”。