ICS 25. 040
CCS N 10

中华人民共和国国家标准

GB/ T 21109. 2— 2023/IEC61511-2:2016
代替 GB/T 21109. 2— 2007

过程工业领域安全仪表系统的功能安全 第 2 部分 :GB/T 21109. 1— 2022的应用指南

Functionalsafetyofsafetyinstrumented systemsfortheprocesindustrysector— Part2:Guidelinesforthe applicationofGB/T 21109. 1— 2022

(IEC61511-2:2016,FunctionalSafety— Safetyinstrumented systemsfortheprocesindustrysector— Part2 : Guidelinesfor the applicationofIEC61511-1:2016,IDT)

2023-03-17发布 2023-10-01实施

国家市场监督管理总局
国家标准化管理委员会 发布

目　　次

前　言

本文件按照 GB/T 1. 1— 2020《标准化工作导则　第 1部分 :标准化文件的结构和起草规则》的规定起草。

本文件是 GB/T 21109《过程工业领域安全仪表系统的功能安全》的第 2 部分。 GB/T 21109已经发布了以下几个部分：

—第 1部分 :框架、定义、系统、硬件和应用编程要求；

—第 2部分 :GB/T 21109. 1— 2022的应用指南；

—第 3部分 :确定要求的安全完整性等级的指南。

本文件代替 GB/T21109.2— 207《过程工业领域安全仪表系统的功能安全　第 2部分 :GB/T 21109.1 的应用指南》,与 GB/T21109.2— 207相比,主要变化如下：

—更改了原 GB/T 21109. 2 的章、条号,在与 GB/T 21109. 1 中对应的章、条号一致的前提下,前面加有符号“A”(见附录 A,更改了旧版的第 1 章 ~第 19章)；

—更改了 A. 12的内容,将原来应用软件要求,包括工具软件的选择准则更改为 SIS应用程序开发的内容(见附录 A. 12,2007年版的第 12章)；

—删除了原附录 A 计算一个仪表安全功能要求时的失效概率的技术示例(见 2007年版的附录 A)；

—更改了附录 B 的内容,将原来附录 B典型的 SIS结构开发更改为使用可靠性框图开发 SIS逻辑解算器应用程序的示例(见附录 B,2007年版的附录 B)；

—更改了附录 C 的内容,将原来附录 C安全 PLC的应用特征更改为从 NP技术转换为 PE技术时的注意事项(见附录 C,2007年版的附录 C)；

—更改了附录 D 的内容,将原来附录 D SIS逻辑解算器应用软件开发方法的示例更改为如何从管道与仪表图(P&ID)演变成应用程序的示例(见附录 D,2007年版的附录 D)；

—更改了附录 E 的内容,将原来附录 E 开发安全配置的 PE逻辑解算器的外配诊断程序的示例更改为用于应用编程的方法和工具(见附录 E,2007年版的附录 E)；

—增加了附录 F:SIS项目示例说明使用继电器梯形图语言开发应用程序的安全生命周期每个阶段(见附录 F)；

—增加了附录 G:应用程序开发实践的指南(见附录 G)。

本文件等同采用 IEC 61511-2: 2016《功能安全　过程工业领域安全仪表系统　第 2 部分: IEC 61511-1:2016的应用指南》。

本文件做了下列最小限度的编辑性改动：

—将标准名称改为《过程工业领域安全仪表系统的功能安全　第 2 部分：GB/T 21109. 1— 2022的应用指南》。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC124)归口。

本文件起草单位 :机械工业仪器仪表综合技术经济研究所、国家管网集团西南管道有限责任公司、中国石油集团安全环保技术研究院有限公司、北京龙鼎源科技股份有限公司、上海辰竹仪表有限公司、北京京仪集团有限责任公司、杭州盘古自动化系统有限公司、北京联合普肯工程技术股份有限公司、济南市长清计算机应用公司、济南宁通自动化技术有限公司。

本文件主要起草人刘瑶、史学玲、周有铮、李玉明、徐德腾、张韬、张建国、朱明露、裘坤、熊文泽、张艾森、魏辰强、陈小华、孙文勇、吴祚祥、靳江红、王玥、张新国、沈玉富、杨柳、姜荣怀、钱福群、周婷、韩占武、马欣欣、帅冰、王莉、张洪、俞文光、程相国、左新、朱弘毅、聂中文、田雨聪、李秋娟、施隋靖、朱旭营 、陈红新 。

本文件及其所代替文件的历次版本发布情况为 ：

— 2007年首次发布为 GB/T 21109. 2— 2007;

—本次为第一次修订 。

引　言

在过程工业中,用来执行安全仪表功能的安全仪表系统已应用多年 。要使仪表能有效地用于安全仪表功能,最重要的是该仪表需达到某些最低标准和性能水平 。

GB/T 21109阐述了过程工业安全仪表系统的应用 。GB/T 21109还强调要执行 一 次过程危险和风险评估(H&RA),使之能导出安全仪表系统的规范 。仅在与安全仪表系统的性能要求相关时,才考虑其他安全系统的贡献 。安全仪表系统包括执行安全仪表功能所必要的从传感器到最终元件的所有设备 。

GB/T 21109拟包括以下几部分：

—第 1部分:框架、定义、系统、硬件和应用编程要求 。　目的是提出安全仪表系统(SIS)的规范、设计、安装、运行和维护要求,以确保该系统能使过程达到或保持安全状态 。

—第 2部分:GB/T 21109.1— 2022的应用指南 。　目的是提供按 GB/T 21109.1— 2022中定义的安全仪表功能及其相关的安全仪表系统的规范、设计、安装、操作和维护的指南 。

—第 3部分:确定要求的安全完整性等级的指南 。　目的是确定安全仪表功能的安全完整性等级的各种不同方法 。

GB/T 21109包含了作为应用基础的两个概念:安全生命周期和安全完整性等级 。

GB/T 21109针对基于使用电气(E)/电子(E)/可编程电子(PE) 技术的安全仪表系统 。　在逻辑解算器使用其他技术的情况下,需应用 GB/T 21109的基本原则来确保实现功能安全要求 。GB/T 21109还涉及安全仪表系统的传感器和最终元件,不管它们用了何种技术 。GB/T 21109在 GB/T 20438的框架范围内专用于过程领域 。

为达到上述最低原则,GB/T 21109提出了 SIS安全生命周期活动的方法 。采纳此种方法以便使用合理和一致的技术策略 。

在大多数情况下,固有安全过程设计就能很好地实现安全性 。但是在某些情况下,这是不可能或不切实际的 。必要时,还可结合一个或一些保护系统来降低已发现的残余风险 。保护系统可依靠不同的技术(化学的、机械的、液压的、气动的、电气的、电子的、可编程电子的)。 为促成该方法,GB/T 21109要求：

— 执行危险和风险评估以便确定整体安全要求；

— 给安全仪表系统分配安全要求；

— 在一个框架内工作,该框架适用于实现功能安全的所有仪表类措施；

—详述如何使用某些活动(如安全管理),这些活动适用于实现功能安全的所有方法 。

针对过程工业的安全仪表系统的 GB/T 21109:

—包括从初始概念、设计、实现、运行和维护直到停用的所有 SIS安全生命周期阶段；

— 能使现有的或新的国家专用的过程工业标准同 GB/T 21109协调一致 。

GB/T 21109致力于在过程工业领域达到高度一致(如基本原则、术语、信息等) 。这将带来安全和经济两方面的好处 。GB/T 21109的整体框架见图 1。

在权限方面,在管理当局(如国家的、省的、自治区的等)已建立过程安全设计、过程安全管理或其他规定的情况下,这些要求需比 GB/T 21109中定义的要求优先考虑 。

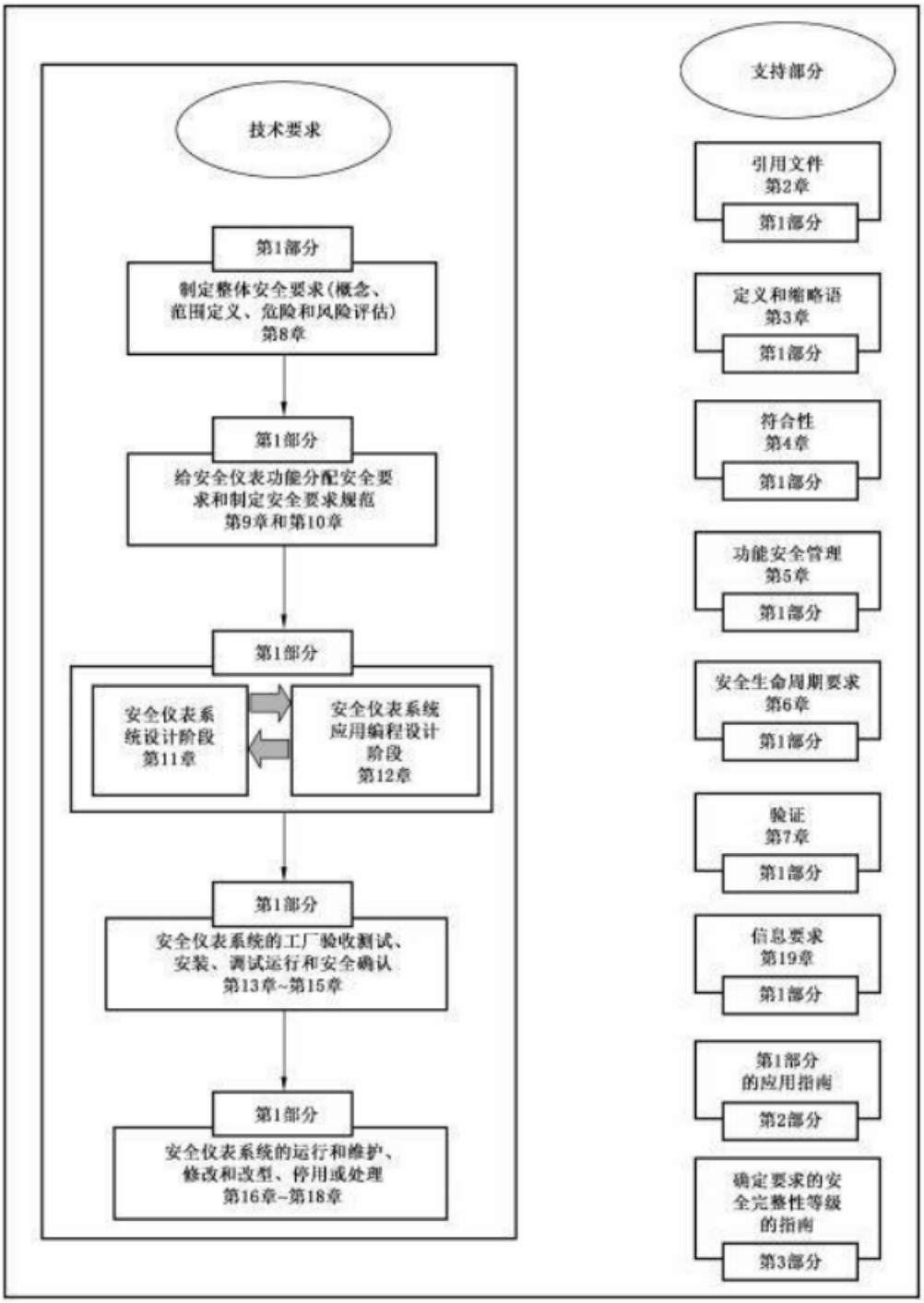


图 1　GB/T 21109的整体框架

过程工业领域安全仪表系统的功能安全 第 2 部分 :GB/T 21109. 1— 2022的 应用指南

1 范围

本文件提供了按 GB/T 21109. 1— 2022中定义的安全仪表功能及其相关的安全仪表系统的规范 、设计 、安装 、操作和维护的指南 。

注 1: 附录 A(资料性)已进行整理 ,其章条号除前面加有符号 “A” 外 ,其余与 GB/T21109. 1— 2022中对应的章 、条号一致 。

注 2: 附录 A包含 GB/T 21109. 2— 2007正文中的材料 ,这样 做 是 为 了 防 止 出 现 标 准 正 文 均 为 资 料 性 条 款 的 情 况 , 以符合标准编写规则 。

注 3: 为了使本文件最大化利用 :

— 在使用特定条款指南时也需要同时回看所属章节指南(例如 : 当查看 5. 2. 6. 1. 3 的指南时 ,也 要 考 虑 5. 2. 6 的指南) ;

— 在特定条款无相关指南时(例如 :未提供进一 步指南) ,在适用时可考虑回看章节指南 。

注 4: 本文件附录中给出的示例仅仅是在具体情况下实施 GB/T 21109要求的特定例子 ,用户可根据自己的情况选择适用的方法和技术 。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款 。其中 , 注 日期的引用文件 ,仅该日期对应的版本适用于本文件 ;不注日期的引用文件 ,其最新版本(包括所有的修改单) 适用于本文件 。

GB/T 21109. 1— 2022 过程工业领域安全仪表系统的功能安全 第 1 部分 框架 、定义 、系统 、硬件和应用编程要求(IEC 61511-1:2016,IDT)

3 术语、定义和缩略语

GB/T 21109. 1— 2022界定的术语 、定义和缩略语适用于本文件 。

附 录 A
（资料性）
GB/T 21109. 1— 2022的指南

A. 1 范围

未提供进一 步指南 。

A. 2 规范性引用文件

未提供进一 步指南 。

A. 3 术语和定义及缩略语

未提供进一 步指南 。

A. 3. 2. 65 安全功能

一个安全功能应能防止 一 个特定的危险 事 件 。 例 如 “防 止 容 器 # ABC456 中 压 力 超 过 10 MPa” 。可以通过下列办法达到这个安全功能 ：

—单独一个安全仪表系统(SIS)；

— 一个或几个安全仪表系统和/或其他的保护层 。

每个安全仪表系统或其他的保护层应有达到安全功能的能力并且整体组合一定要达到要求的风险降低(过程安全目标) 。

A. 3. 2. 66 安全仪表功能

安 全仪表功能(SIF)源于安全功能 ,安全仪表功能具有 一个相关联的安全完整性等级(SIL)并由 一个特定的安全仪表系统(SIS)来执行它 。例如 “当容器 #ABC456中的压力达到 10MPa时 ,在 5 s 内关闭 阀门#XY123” 。多个安全仪表功能(SIF)有可能使用同一个安全仪表系统(SIS)的设备 。

A. 4 与 GB/T 21109. 1— 2022的符合性

未提供进一 步指南 。

A. 5 功能安全管理

A. 5. 1 目的

未提供进一 步指南 。

A. 5. 2 “要求” 指南

A. 5. 2. 1 概述

当一个组织负责执行功能安全所必需的一项或几项活动 ,并且该组织按照质量保证规程进行工作时 ,则出于质量的目的 ,GB/T 21109. 1— 2022第 5 章中描述的许多活动将要被执行 。在这种情况下 ,对功能安全来说 ,没有必要重复这些活动 。但宜对质量保证规程进行复审 ，以确定它们对达到功能安全目标是合适的 。

A. 5. 2. 2　组织和资源

宜定义一个公司/现场/工厂/工程项目范围内与安全仪表系统(SIS) 有关联的组织结构，并清楚地了解和沟通每个人员/部门的角色和职责 。宜确定结构内的各个角色，包括他们的描述和目的 。宜明确每个角色的责任及各自的具体职责 。此外，还宜标明各个报告提交给谁和委派谁来写报告 。　目 的是保证组织中的每一个人都要了解他们对安全仪表系统(SIS)而言所扮演的角色以及他们的职责 。

宜确定为实现与安全仪表系统(SIS)有关的安全生命周期的所有活动所需的技能和知识;并确定每种技能所要求的能力水平 。宜根据可胜任的每种技能以及每种技能所需的人数对资源进行评估 。　当查明有差异时，宜制定一个开发计划使之能及时地达到要求的胜任能力水平 。所有人员都宜始终在岗，以维持生命周期背景以及经验的传递 。　当出现技术力量短缺时，可招收或签约合格的有经验人员 。

A. 5. 2. 2. 1　未提供进一步指南。

A. 5. 2. 2. 2　未提供进一步指南。

A. 5. 2. 2. 3　未提供进一步指南。

A. 5. 2. 3　风险评价和风险管理

GB/T 21109. 1— 2022的 5. 2. 3 中规定的要求是确定危险 、评价风险并确定必要的风险降低 。公认的进行这些评价的适用方法有很多种 。GB/T 21109. 1— 2022并未指定任何 一 种特殊的方法 。进 一 步指南见 A. 8. 2. 1。

A. 5. 2. 4　编制安全计划

本条目的是要保证在整个项目范围内，实施适当的安全计划编制以便论述生命周期每个阶段所要求的活动(例如工程设计 、工厂运行) 。GB/T 21109没有针对计划编制活动提出特殊的组织结构要求，但它强调要求定期更新或复审这些活动 。

A. 5. 2. 5　执行和监视

A. 5. 2. 5. 1　GB/T 21109. 1— 2022的 5. 2. 5. 2 的目的是要确保有效的管理规程能到位从而：

—保证危险分析 、风险评估 、其他评估和审核活动 、验证和确认活动产生的建议得以圆满解决 。

— 确保 SIS在它的整个工作寿命期内都能按安全要求规范(SRS)运行 。

A. 5. 2. 5. 2　在本文件中，供应商可能还包括设计承包商和维护承包商以及设备供货商 。　SIS组件的硬件和软件均宜根据被认可的质量管理体系如 ISO 9000系列标准制造 。

宜定期对 SIS的性能进行复审，以保证始终遵守原来在 制 定 安 全 要 求 规 范(SRS) 过 程 中 的 设 想 。例如，宜对 SIS中的各个设备假设的失效率进行定期的复审，以保证它保持同初始定义相同 。如果失效率比初始预计的更差，则可能要修改设计 。　同样还宜对 SIS的要求率进行复审 。如果对 SIS的要求率大于最初假定值，则可能需要对 SIL进行调整 。

A. 5. 2. 5. 3　未提供进一步指南。

A. 5. 2. 5. 4　未提供进一步指南。

A. 5. 2. 6　评估、审核和修订

评估和审核是以误差检测和消除为目标的手段 。后续段落阐明了这些活动之间的差别 。

功能安全评估的目的是评价在所评估的各生命周期阶段中为实现安全所做的准备是否充分 。评估者宜对负责实现功能安全人员所作的决定做出判断 。例如 :在调试运行之前宜对维护规程是否充分做一次评估 。

功能安全审核人员宜通过工程项目记录或者工厂记录来确定必要的规程是否已由具有必要能力的

人员以规定的频率执行 。不要求审核人员对他们考虑的工作的充分性做出判断 。然而 ,如果他们发觉更改有益 ,则宜在报告中包括对此的说明 。

在许多情况下 ,评估人员和审核人员的工作之间有可能重叠 。例如 ,不论评估人员还是审核人员可能不仅需要确定操作员是否已得到必要的培训 ,而且还要对培训是否使操作员达到了要求的能力做出判断 。

A. 5. 2. 6. 1 功能安全评估

功能安全评估(FSA)是证明安全仪表系统(SIS) 满足安全仪表功能(SIF) 要求和安全完整性等级(SIL)要求的基础 ,安全仪表系统可能用到 一 个或多个应用程序 。 这种评估的基本 目 的是通过系统开发过程的独立评估来证明符合一致同意的标准和惯例 。在各个生命周期阶段 ,可能都需要对 SIS进行评估 。为了进行有效的评估 ,宜拟定一个定义该评估范围的规程以及评估小组组成的指南 。

FSA 的良好实践需考虑以下属性 。

a) 对每个 FSA都宜拟制一个计划 ,这个计划宜根据评估范围 、评估人员 、评估人员的能力以及评估将产生的信息来制定 。

b) FSA宜考虑其他标准和实践 ,这些标准和实践可能包含在外部或内部企业标准 、指南 、程序或实践准则中 。FSA计划宜定义对于特定的评估/系统/应用领域评估的内容 。

c) 在不同的系统开发过程 ,功能安全评估的频次可能改变 ,但至少在系统面临危险之前宜进行 一 次 FSA。有些公司也可能在施工/安装阶段之前进行 一 次评估 ,以防止在生命周期的较后阶段出现高成本的返工 。

d) 在定义 FSA频次和严格程度时宜考虑以下系统属性 :

- 复杂程度;
- 安全重要性;
- 类似系统以往的经验;
- 设计特征的标准化 。

e) 在评估之前宜提供足够的设计 、安装 、验证和确认活动的证据 。足够证据的可用性本身可能是一个评估准则 。证据宜代表系统设计或安装的现状/认可状态 。

- 评估者的独立性一定要合适 。
- 评估者宜具有适合于所评估系统的技术和应用领域的经验和知识 。
- 在整个生命周期和对所有系统而言 ,实现 FSA 的方案都宜保持系统性和 一 致性 。FSA是一种主观的活动 ,为了尽可能多地消除主观性 ,可以使用检查表来定义 一 个组织可接受活动的详细指南 。
- 审查技术 ,用于核实应用程序(AP)功能达到过程危险要求 。
- 功能测试 ,用于核实 AP执行了所要求的功能 ,并尽可能显示 AP或嵌入式软件中的附加功能不会造成危险情况的发生 。
- 结构测试(见 A. 12. 5. 3) ,用于核实 AP在必要的时间内执行所要求的功能 ,并确定 AP是否存在未测试部分 ,这些部分(由于未经过测试)可能会造成危险情况的发生 。
- 功能失效分析和假设分析(whatif) ,用于核实 AP功能不会导致危险状态 。
- 规程已制定 ,用于核实受控开发和验证过程已就位 ,并显示所使用的 AP版本和嵌入式软件版本都是正确的 。
- 审核规程和计划表已制定 。

FSA产生的记录完整 ,并且在生命周期下 一 阶段开始之前 ,评估结论宜同负责 SIS功能安全管理人员的意见一致 。

为了增强评估的客观性 ,需要独立于项目组的评估人员 。需要高级(例如 ,经验 、职位)评估人员 ,以

保证他们所关心的问题能被适时地关注和涉及 。如 GB/T 21109. 1— 2022 中 5. 2. 6. 1. 3 注 中 进 一 步 建议 ,对于某些大型项目组或评估小组 ,可能有必要拥有多个独立于原项目组的高级人员 。

根据公司组织结构和公司内部专业技术能力 ,也许不得不通过外部组织来满足对独立评估人员的要求 。相反地 ,如果公司有与负责项目的人员(从管理和其他资源方面)独立且分开的内部组织 ,并且该组织能够熟练地进行风险评估和 SIS应用 ,那么公司可使用此类内部组织的资源来满足对独立组织的要求 。

评估工作量与工程项目的规模和复杂程度有关 。在同一 时间可以对不同阶段的结果进行评估 。在役装置有少许变更情况下尤其可能 。

在某些地区 ,在阶段 3进行的功能安全评估常被称为开车前安全审查(PSSR) 。

见表 F. 1框 10。功能安全评估的职责范围宜在安全计划期间商定 。

评估小组宜能获取他们执行评估所需要的任何信息 。这包括从 H&RA,设计阶段 一 直到安装 、调试运行和确认阶段得到的信息 。

A. 5. 2. 6. 1. 1 在某些情况下 ,功能安全评估小组可以是 一 个人 ,只要 这 个 人 拥 有 该 活 动 所 需 的 技 能 和经验 。

A. 5. 2. 6. 1. 2 评估小组中能胜任的高级人员的数量可能会由于应用场景的大小 、所包含的技术 、沟通要求(例如 :用户/业主 、集成商 、厂商)和项目时间的不同而改变 。

能胜任的高级人员 宜 能 够 胜 任 应 用 场 景 所 包 含 的 各 种 技 术 、适 用 的 法 规 ,并 能 够 满 足 项 目 进 度要求 。

A. 5. 2. 6. 1. 3 未提供进一 步指南 。

A. 5. 2. 6. 1. 4 未提供进一 步指南 。

A. 5. 2. 6. 1. 5 未提供进一 步指南 。

A5. 2. 6. 1. 6 在 SIS的设计 、开发 、运行和维护过程中所用的工具可能会由于在最终系统中引入故障而影响 SIS的完整性 。这些工具可能使工具功能的 一 部分直接 “嵌入” 到 SIS中(例如 ,用户库 、解释器) ,也可成为 “离线” 工具 ,即用于生成可单独检查的信息(例如 ,字段变量计算工具 、测试工具) ,还可成为与正在运行的 SIS连接的工具 ,例如维护工具 。在各种情况下 ,了解潜在的失效模式和影响及其控制手段是非常重要的 。控制工具故障的最典型方法包括 :

- 确认向国家和国际标准的可追溯性(可能包括与工具性质有关的校准和/或功能标准) ;
- 考虑用户经验和以往使用该工具的历史证据;
- 对使用该工具所得出的结果进行复审和功能测试;
- 开发和/或测试工具的多样性— 例如 ,使用来 自不同编译器的代码 ,通过使用不同类型的检验工具检测设计工具的输出;
- 工具作为 GB/T 20438. 2— 2017和 GB/T 20438. 3— 2017设备的组成部分一起提供 。

FSA活动宜检查为保持工具输出的完整性而采取的策略 ,不论是 “嵌入” 工具还是 “离线” 工具 ,并对工具是否已经达到必要水平做出判定 。

A. 5. 2. 6. 1. 7 未提供进一 步指南 。

A. 5. 2. 6. 1. 8 未提供进一 步指南 。

A. 5. 2. 6. 1. 9 未提供进一 步指南 。

A. 5. 2. 6. 1. 10 未提供进一 步指南 。

A. 5. 2. 6. 2 功能安全审核和修订

a) 审核类别

SIS的审核可给工厂管理 、仪表维护工程师和仪表设计工程师提供有用的信息 ,使管理具有前瞻性 ,并使其了解 SIS的实现程度和有效性 ,审核类型有多种 。 任何活动审核的实际类型 、范

围和频率宜反映该活动对安全完整性的潜在影响 。
审核类型包括：

- 检查;
- 安全巡视(例如工厂巡检和事故复审)；
- SIS调查(问卷调查) 。

宜区分“监督和检查”以及审核活动。监督和检查的重点在于评价特定生命周期活动的性能(例如在设备恢复工作之前 ,监督人员检查维护活动的完成情况) 。相反，审核活动更广泛 ,并且主要集中在与安全生命周期有关的整个 SIS的实施上 。审核要包括确定是否执行了监督和检查程序 。
审核和检查可由公司/现场/装置/项目的人员来执行(如 自审)，或由独立人员来执行(如公司的审核员 、质量保证部门 、监管人员 、客户或者第三方) 。
各级管理可能会使用相关类型的审核，以获取 SIS实施的有效性信息 。来自审核的信息可识别出没有被正确应用的规程 ,从而改进实施 。

b) 审核策略

现场/工厂/项目实施审核的程序可以考虑滚动 、独立或者自审和检查程序 。
定期更新滚动程序，以便反映以往 SIS的性能和审核结果，以及当前关心的问题和重点 。这些包含了在一个适当的时段内和适当深度上 ,现场/工厂/项目有关 SIS的所有活动和方面 。
审核的主要原因及其附加价值在于对提供的信息及时采取行动 。这些行动的 目 的是增强 SIS的有效性 。例如 ,有助于降低雇员或公众成员受伤害或致命的风险 、有助于提高安全文化 、有助于防止任何宜避免释放的物质进入环境 。
总之 ,审核策略可能融合了各种审核类型，由管理(客户) 发起，目 的是把相关信息反馈给管理链以便及时采取行动 。

c) 审核过程和协议

目的是建立 GB/T 21109. 1— 2022的符合度并最大化审核的效能 。仅当各方(包括审核者 、联络员 、工厂经理和部门负责人等)理解每个审核的需求并对审核产生影响 ,才能达到最大效能 。以下审核过程和协议也许有助于确保达到上述目的的方案的某种一致性 。它们涉及审核过程的 5个关键阶段 。

1) 审核策略和程序

— 宜清楚地定义每次审核的目的并确定审核组及其任务和职责;
— 宜有审核策略;
— 宜有审核程序;
— 宜对审核过程 、程序和策略执行情况进行定期复审 。

2) 审核准备和前期计划

— 开始进行某次审核之前 ,现场/工厂/项目的高级经理和/或适当的审核协调员宜确定一位联络员 。
— 审核人员和联络员宜尽早对以下问题进行讨论 、理解并达成一致：
  - 审核的范围;
  - 审核的时间安排;
  - 参加的人员;
  - 审核的依据或者审核标准;
  - 为成功完成审核在准备阶段要做的额外工作和涉及到的工厂人员 。
— 以下各项可用作每个阶段所需时间的指南 。
  - 审核准备 :30%;

- 进行审核 :40%;
- 审核结果报告 :20%;
- 审核跟踪 :10% 。

— 审核人员收集信息 、规程/指导书 、数据，以及在适当的时候编制检查表，以准备实施审核。

— 如果发现严重的问题/缺陷，审核人员宜重点关注 并 说 明 审 核 范 围 发 生 变 更 的 可 能程度 。

3) 实施审核

— 审核人员宜在对现场/工厂/项目人员可能造成的影响具有足够的认识后 ,在设定的审核时段内的几组连续工作 日 中实施审核 。

—对在审核过程中已确定的审查结果，宜定期向联络员通 报，以 免 在 审 核 结 束 时 感 到意外 。

— 在审核过程中 ,审核人员宜尽量让工厂人员参与审核过程，以传授对过程的学习和理解 ,使工厂人员对审核结果有所了解 。

— 审核人员的风格对审核的成功是决定性的— 他要努力做到有耐心 、态度积极 、有礼貌 、精力集中和客观 。

— 至少审核人员要尽量在协商后改变商定好的范围和时间表 。

4) 审查结果报告

— 在审核结束时或晚些时候 ,但宜在发布最终报告之前 ,审核人员组织末次会议 。

— 宜给相关的管理部门对草案报告和审查结果提意见的机会 ,如有要求可在末次会议上进行讨论 。

— 通常做法是由现场/工厂/项目提供一份针对报告结果的整改行动计划 。

5) 审核跟踪

— 审核报告通常需要以行动计划的形式做出响应 。 只要合适，审核人员可在预定 日期或者下次审核时 ,验证整改行动的完成度 。

— 现场/工厂/项目跟踪系统可用来检查行动计划的执行 。

— 宜对每个审核组的审核结果考虑定期复审/总结 ,并就其结果进行广泛沟通 。

— 审核结果/输出可用于确定审核的频次 ,并可用于 SIS的管理评审的输入 。

A. 5. 2. 6. 2. 1 未提供进一 步指南 。

A. 5. 2. 6. 2. 2 功能安全审核可由公司/现场/装置/项目自己的员工执行(例如自审) ,或者由独立的人员执行(例如公司审核人员、质量保证部门、监管人员、客户或第三方) 。关于进一步指南 ,见 GB/T 20438.1— 2017中的表 4和表 5。

A. 5. 2. 6. 2. 3 GB/T 21109. 1— 2022中第 5. 2. 6. 3、5. 2. 6. 4 和 5. 2. 6. 5 条强调变更管理在审核过程中的作用 。如果最初的风险分析把 BPCS或操作规程中的非 SIS保护层作为有效的风险降低措施 ,则宜对这些系统发出的报警和所做的更改进行监测，以确保它们不会降低非 SIS保护层所提供的保护作用 。此外，即使对 SIS或接口系统中的版本变化或修改量非常小 ,也可能导致 AP、嵌入式软件和硬件之间出现不兼容的情况(例如 ,设想返回到老版本的软件程序是多么的困难) 。 因此 ,确保子项受控的同时项目总体配置也受控是非常重要的 。尤其是 AP和软件版本必须与硬件版本 、操作规程以及为其设计的专用接口一致 。

A. 5. 2. 6. 2. 4 未提供进一 步指南 。

A. 5. 2. 7 SIS配置管理

A.5. 2. 7. 1 为了在整个生命周期内管理和保持设备的可追溯性 ,可以建立一种用于标记 、控制和追踪每个设备的型号/版本的机制 。

宜在安全仪表系统安全生命周期尽可能早的阶段 ,给每台设备建立唯一 的标识 。在某些情况下 ,也

可保留和控制仍在使用中的较早型号/版本 。这只是配置管理程序中的第一 步 ,配置管理程序还包括以下考虑 。

配置管理系统可以包括下列内容 。

a) 制定所有设备在生命周期内的标识规程 。

b) 每台设备包括嵌入式系统 、工具软件和 AP 的型号/版本以及生成状态的唯 一 标识 ,包括供货商 、日期和适用时最初规定的型号/版本的变更情况 。

c) 识别和跟踪由故障观察和审核引起的所有行动和变化 。

d) 对投用版本的控制 ,识别出相关设备的状态及型号/版本 。

e) 设置安全防护措施，以确保在运行中的 SIS不会遭受未经授权的变更/修改 。

f) AP每个部分的版本标识 ,这些部分共同构成了完整 AP的一个特定版本 。

g) 提供在一个或多个装置中多套 SIS更新的协调方案 。

h) 投入使用的书面授权 。

i) 批准设备投入使用的签批的列表 。

j) 设备被纳入配置控制的阶段 。

k) 对相关交付文档的控制 。

l) 在以下规范中确定设备的型号/版本：

- 功能规范;
- 技术规范 。

m) 变更管理规程的使用 。

宜确定 SIS的管理和维护涉及的所有部门/组织 ,为其分配职责并使其知晓 。

原则上 ,AP配置管理的要求与系统硬件设备的相关要求相同 。然而 ,与纯硬件设备使用的方法相比 ,AP通常采用更加严格的方法，因为：

- AP固有的“逻辑”特性而非“物理”特性使得其实际配置难以“观察”，而需要通过参考其支持文件;
- 它易于修改(对于程序员来说 ,一天内发布几个不同的版本并不罕见)；
- 应用的功能性完全依赖于 AP功能的正确执行，因此 ,其正确性是整个 SIS正确运行的关键;
- 它可随着 PE系统的版本不同 ,外部接口的变化 、输入和输出数据范围的不同 、甚至自主开发工具版本的不同而表现不同;
- 它可因特定的规范集 、构建配置 、SIS子系统 、环境和位置而异 ,需要通过它的配置管理版本和修订来区分 。

除用于标识 、版本和修订控制以及子项之间兼容性的标准配置管理要求外 ,还宜包括下列用于维护控制 AP的典型因素：

- 在 AP中使用嵌入代码 ,确保其只能被下载到 目标硬件主机中(在不同场合中可使用多个不同配置的地方尤其有用)；
- 在新程序版本可以下装到 SIS之前 ,使用需要经过一个或多个指定机构授权的发布说明;
- 在 AP开发 、测试和维护过程中使用的所有项状态和版本维护记录可追溯至与整体配置关联的相关规范和验证结果;
- 维护备份 ,使系统能恢复至原有构建;
- 使用受控的修改周期 ,从而将这些修改置于定义好的版本中 ,有利于在不同的成熟阶段开发不同的版本 ,不同版本之间不会相互影响 ,且测试周期也能保持某 一 特定版本在发布到现场之前的稳定性水平 。

A. 5. 2. 7. 2 未提供进一 步指南 。

A.6 安全生命周期要求

A.6.1 目的

任何过程设施中所达到的功能安全,都有赖于一系列活动的圆满执行。针对SIS采用系统性SIS安全生命周期方法的目的,是确保能执行达到功能安全所必要的全部活动,以及保证能向其他人证明已按适当顺序执行了这些活动。在GB/T 21109.1— 2022的图7和表2中提出了典型的生命周期。在GB/T 21109.1— 2022的第8章~第18章中给出了每个生命周期阶段的要求。

GB/T 21109认为如果遵守所有的要求,那么可以用不同的方法构建规定的活动。如果能够将安全活动更好地整合到正常的项目程序中,这种重构将是有益的。GB/T 21109.1— 2022的第6章的目的是当使用不同的SIS安全生命周期时,确保已定义了生命周期每个阶段的输入和输出,及所有最基本的要求。

A.6.2 “要求”指南

A.6.2.1 考虑的关键是事先定义好SIS安全生命周期。经验表明,除非事前对该活动作了很好的计划,并且所有人员、部门和组织对承担的职责达成一致意见,否则有可能发生问题。出现问题时,最好的情况是某些工作被延误或不得不重做;最糟糕的情况是可能影响安全。

宜明确每个生命周期阶段中的责任层级,并与相关各方(例如分项供应商、系统集成商、最终用户)进行沟通,让各方明确职责、与其他方活动和安全生命周期阶段之间的关系,以及他们交付的成果对整体功能安全和安全完整性要求有着怎样的影响。

A.6.2.2 虽然并不是一个要求,但是在早期阶段把建议的SIS安全生命周期(包括适用于项目的GB/T 21109.1— 2022图7中的方框)映射到过程的项目生命周期之中,是有好处的。当这样做时,宜考虑开始某个安全生命周期活动所需的信息以及谁能提供这些信息,以便将SIS安全生命周期责任分配给特定人员。在某些情况下,直到设计阶段的后期,都不可能精确确定某个特殊问题的相关信息。此时,有必要根据以往经验进行估计,在后期再证实这些数据,在SIS安全生命周期中注意这点很重要。

A.6.2.3 SIS安全生命周期计划编制的另一重要部分是识别每个阶段将使用的技术。确定这些技术是重要的,因为通常需要使用专门的技术,这种技术要求人员或部门具有特定的技能和经验。例如,在某个特定应用中的后果可能与失效事件发生后产生的最大压力有关;能够确定这种关系的唯一方法就是建立过程的动态模型。因此,动态建模的信息要求将对设计过程有重大影响。

A.6.2.4 由于详细的设计、验证、确认和测试证据产生于其他安全生命周期阶段,因此在发生任何变更后,证实安全生命周期的每个阶段仍然保持一致、未引入新的危险、应用仍然按要求运行是非常重要的。

A.6.3 “应用程序SIS安全生命周期要求”指南

A.6.3.1 AP的SIS安全生命周期始于SIS安全生命周期的第3阶段(SISSRS),止于第3阶段FSA。

如果AP安全生命周期满足GB/T21109.1— 2022表3的要求,则可以根据项目的安全完整性和复杂性,调整V模型(见图A.1)各阶段的深度、数量和规模。

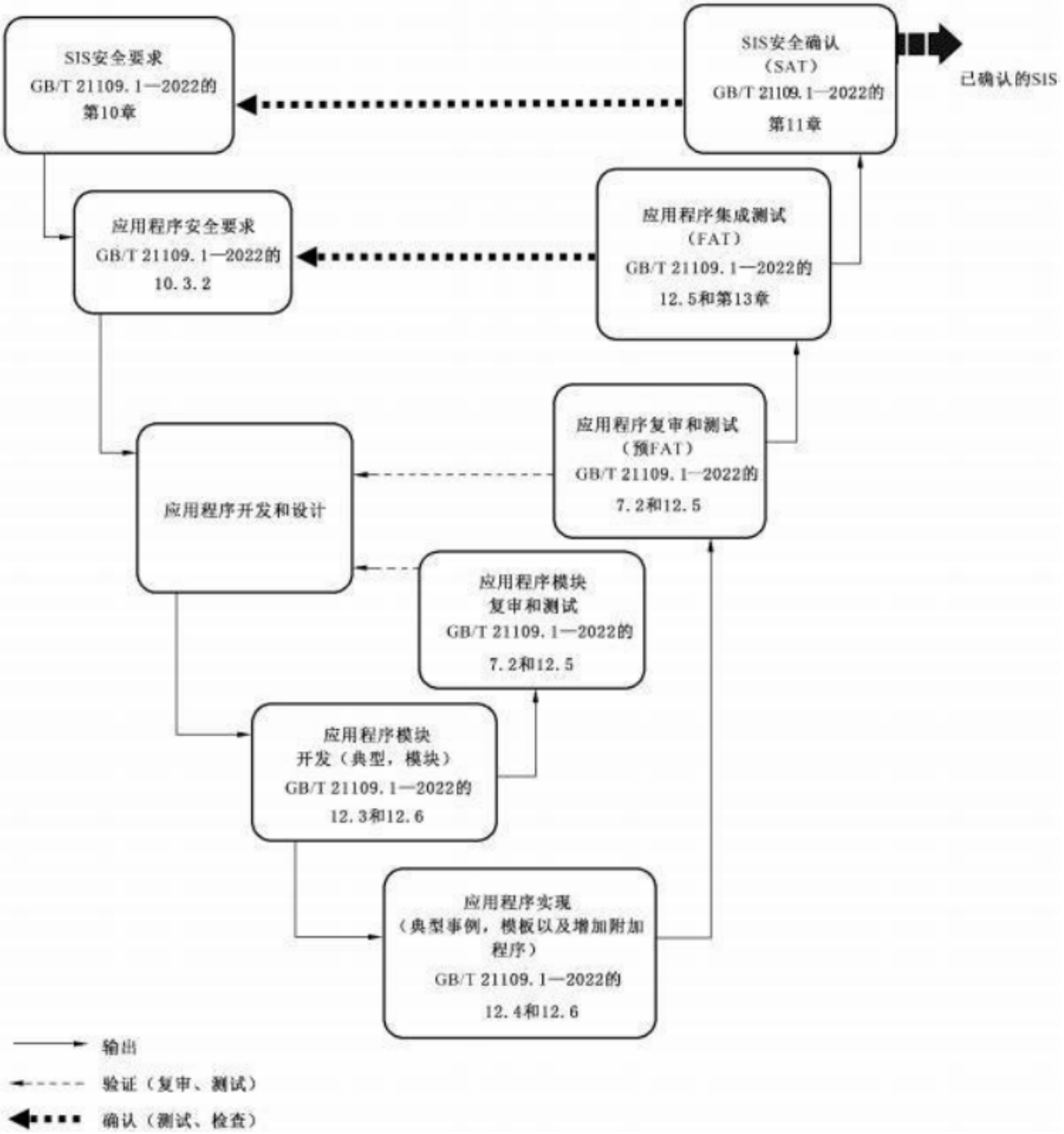


图 A. 1 应用程序 V模型

所用 AP语言的类型以及语言与应用功能的紧密性可能会影响 V模型阶段的范围 。例如，当 LVL (如 GB/T 15969. 3— 2017梯形图或功能块图)用于 AP的设计 、实现 、验证和确认时，只有两级标准 AP "V" 模型可用：

- "V" 模型中 "应用模块开发" 可理解为新功能的设计和实现;
- "应用模块测试" 可理解为新功能的验证和测试 。

在使用 FVL开发新功能并由此需要提供更详细的 AP(即软件代码) 开发过程的情况下 ,开发人员宜遵循 GB/T 20438. 3— 2017 中定义的所有生命周期阶段和规程。 可将 AP SRS作为一部分纳入 SISSRS。

A. 6. 3. 2 方法和技术的选择宜考虑具体的情况 。影响这一决定的因素可能包括：

- AP的规模;

- 复杂程度;
- 需要实现的 SIF的 SIL;
- 设计工具(例如配置工具)的标准化程度;
- 应用程序的语言类型(例如附录 B 中的功能块;图 D. 2 和表 F. 14中的因果图;图 F. 11中的继电器梯形图) 。

见 A. 12. 6. 2 中的方法和技巧示例 。

A. 6. 3. 3 未提供进一 步指南 。

A. 7 验证

A. 7. 1 目的

验证的目的是要保证验证计划编制所确定的每个 SIS安全生命周期阶段的活动实际上已得到执行 ,并保证阶段的输出(无论是文档形式 、硬件或 AP形式)已被产生且适合作为阶段交付物 。

A. 7. 2 “要求”指南

A. 7. 2. 1 GB/T21109. 1— 2022已考虑各个组织将有它们自己的验证规程 ,并且并不总是要求以同样的方式执行这些规程 。换句话说 ,GB/T 21109. 1— 2022第 7 章的 目 的是事先就计划好所有的验证活动 ,以及要使用的规程 、措施和技术 。

A. 7. 2. 2 为了揭示并消除 AP中已经存在的故障 ,需要在整个开发生命周期内进行验证 。 总之 ,为了保证可测试性 ,建议在设计和开发阶段考虑 AP集成测试规范 。测试的范围可参考以往执行过的测试 。

在 AP开发周期(包括测试)的每个不同阶段 ,验证宜证实该阶段已顺利完成 。一 般来说 ,验证根据应用的需要 ,通过一人或多人组成的验证来完成的 。

为了减少由于先入为主的思维定式而产生的错误 ,验证活动宜由合格人员执行 ,该人员未参与编写应用代码 。对于 SIL3的应用 ,则由拥有独立汇报途径的人员执行验证 。

在 AP开发工具包括某些自动验证操作[例如检查位号(命名变量) 的重复使用]的情况下 ,验证小组宜确认工具得以正确使用 ,并确认所获得结果的正确性 。

对于所有的 SIL,建议测试范围包括所有 AP SIF和 SIS失效响应(例如供电失效 、处理器失效 、输入硬件失效 、输出硬件失效以及通信失效) 。但为了进 一 步减少遗留在 AP 中的任何错误 ,建议执行以下附加测试 :

- 基于内部结构的测试(例如内部算法 、内部状态) ;
- 压力测试(例如输入变量和内部变量的异常范围条件 、异常的输入组合 、异常顺序和加载) 。

对于所有的 SIL建议 ,验证和测试文件显示验证和测试已经执行并成功 。此外 ,还建议 :

- 文件允许对验证和测试的充分性进行评估;
- 文件允许独立人员重复测试并复审能达到的覆盖范围 。

数据验证包括证实 AP中所用的数据是正确的 ,并证实在适当的情况下是唯一 的[例如位号名称是唯一分配的 ,数据不会被后续功能误用以及常数(如警报设置点)是有效和正确的] 。

对未授权变更的保护作用进行验证 ,包括验证机制的存在(例如具有访问权限的密码保护) ,并已经充分运用了这些机制 。

一个过程系统可能含有符合不同标准(例如关于机械的GB 28526— 2012以及关于燃烧器的NFPA 85:2015)的一个或多个嵌入式系统 。这要求对硬件 、AP 以及嵌入式软件进行仔细地集成 。 实现这点的一种方式是将非过程系统[即必须符合其他标准(如机械 、燃烧器等)的系统]视为过程设备进行 H&RA, 以确保识别所有潜在的危害 ,并提供已确认的附加保护措施 。

A. 7. 2. 3 未提供进一 步指南 。

A. 7. 2. 4　未提供进一步指南。

A. 7. 2. 5　当 AP进入验证和测试生命周期阶段时，对于 AP进行任何修改或变更会使前一阶段中形成的证据无效。在这种情况下，可能的方法是，可从头开始重复整个生命周期，但这耗费很大，不仅会导致项目延迟，还几乎会在所有情况下增加许多不必要的工作。另一种方法是使用影响分析，辨识出可能已经受到影响的区域，然后集中精力保证这些区域重新得到确认。

A. 7. 2. 6　验证结果是重要的，这样可以证明在 SIS安全生命周期的各个阶段都已进行了有效的验证。

A. 8　过程危险和风险评估

A. 8. 1　目的

本章的总体目的是确定用以保证过程安全所需的安全功能和其相关的目标失效量。安全功能根据 GB/T 21109. 1— 2022第 9章节分配到保护层。在过程领域中，使用多个保护层是常见的，这样在某一层失效时才不会导致或可能产生有害的后果。在 GB/T 21109. 1— 2022 的图 9 中显示了典型的保护层。

A. 8. 2　“要求”指南

A. 8. 2. 1　对 H&RA 的要求是根据结果来规定的。这意味着组织可以使用其认为有效的任何技术，只要该项技术能清楚描述安全功能和其相关的目标失效量。

H&RA宜识别和处理在所有合理的可预见的情况下(包括故障工况和合理的可预见的误用) 发生的危险事件。宜考虑以往发生的事件，包括原因、系统失效和经验教训，以防止类似事件再次发生。

就过程领域的典型工程项目而言，宜在基本过程设计的初期就进行初步的 H&RA。在此阶段假设通过固有安全原理以及良好的工程实践的应用(在 IEC 61511的范围内不包含这种降低危险的活动)，已把危险消除掉了或者已把危险降低到了合理可行的程度。对 SIS而言，这种初步的 H&RA是很重要的，因为确立、设计和实现一个 SIS是复杂的任务，需要占用相当长的时间。尽早了解这个工作的另一理由是在完成过程和仪表图之前需要系统架构方面的信息。

一般只要完成了过程流程图和提供了所有的原始过程数据，启动初步H&RA的信息就足够了。宜认识到当进行详细设计时，可能引入附加危险事件。因此，一旦完成了管道和仪表图，还有必要进行一次最终的 H&RA。一般这个最终的分析使用一个正式的和全文档化的规程，如危险和可操作性研究(HAZOP见 GB/T 35320— 2017)。宜证实所设计的保护层足以管理工厂的风险。在该最终分析期间，需考虑保护层的失效(或保护层成功动作)是否会导致任何新的危险事件或者要求。如果在此阶段确定有任何新的危险事件，则有必要定义新的安全功能。另一个可能的问题是又辨识出导致危险事件发生的其他原因，该危险事件是由初始阶段辨识出的。于是需考虑是否需要对初始分析所确定的安全功能及其目标失效量要求进行修订。

用来确定危险事件的方法取决于应用场合，对有些简单的过程来说，在对一种标准设计(如海上钻井平台)具有大量操作经验的情况下，使用行业上编制的检查表(例如 ISO 10418:2003和 APIRP14C:2001中的安全分析检查表)可能是足够的。在考虑更复杂的设计或是新的过程设计的情况下，有必要采用更严谨的方法(例如 ISO 31000:2009)。

注：ISO 17776:2000中给出了有关选择合适技术的其他信息。

当考虑特定危险事件的后果时，宜考虑所有可能的结果，及对结果产生影响的危险事件的频率。不能忽略或遗漏可信的后果。例如，使管道或压力容器承受超过设计的压力并不一定会产生灾难性的泄漏。在许多情况下，设备都经过高于设计压力的试验，唯一的后果可能是可燃物质泄漏导致火灾。在评价后果时，需咨询负责工厂机械完整性的人员。他们不仅考虑原始试验压力还考虑包括原始设计是否包含腐蚀允许量以及腐蚀管理程序是否到位。在后果是基于这些假设的情况下，清楚地说明这个问题

是很重要的,这样就能把相关的规程结合到安全管理系统中 。

当考虑后果时,另外一个问题是可能会受到某种特定危险的影响的人数 。许多情况下,操作和维护人员只是偶尔在危险区域出现,在预测后果时可考虑到这 一 点 。在使用这种统计方法时宜注意并非对所有的情况都有效,比如在开车期间可能发生危险事件,此时人员频繁出现在危险区,还宜考虑到由于在事件的发生过程中要进行现场检查,所以在危险事件附近出现的人数还可能增加的情况 。

宜对预期过程操作模式进行评估,如开车 、连续运行 、停车 、维护和定期清理 。宜考虑对 SIS提出的合理的可预见的要求,例如在预期过程操作模式下出现的设备失效,控制系统 、其他保护层 、维护错误,手动干预(如 BPCS手动控制功能)以及公用工程丧失(如空气 、冷却水 、氮气 、供电 、蒸汽 、伴热等) 。

当考虑要求频率时,在某些复杂情况下,可能有必要进行故障树分析 。仅在因多个事件的同时失效(或相继隐蔽失效)而产生严重后果的情况下是必要的(例如未考虑所有泄压的最坏情况设计泄压总管),需对什么时候操作员错误宜被视为已识别危险事件的始发原因,以及这种事件发生的频率做出判断 。还需注意的情况是需要通过采信操作员动作以降低要求频率的场合 。这种可信度会受到人为因素(比如采取动作需要多快)和涉及任务的复杂程度的限制 。 当声明的操作员动作可信度 >10时,宜进行人因可靠性分析 。如果声明的风险降低 >10,则系统宜根据 GB/T 21109. 1— 2022进行设计 。 承担安全功能的系统包括检测危险工况的传感器 、报警显示 、人员响应以及操作员用来消除任何异常情况的设备 。声明的风险降低 ≤10时无需遵守 IEC 61511,这时宜仔细考虑人为因素问题 。如果对报警保护层声明了风险降低,需基于以下方面的支持 :对该报警必要响应的文档化描述,足以供操作员采取正确动作时间的判断,采取预防动作的操作员的培训保证(初始培训和再培训) 。

报警系统可以通过降低 SIS的要求率作为风险降低的手段,或者可用作降低场景中整体风险的独立保护层安全功能 。报警系统的设计需考虑如下几个方面 。

- 当控制失效导致对报警系统的 一 次要求时,报警系统的传感器以及对这 一 过程采取动作的最终元件不可用于控制功能,除非分析表明总体风险可接受 。宜关注共同原因和共同模式问题 。
- 报警系统的传感器以及对这 一 过程采取行动的最终元件不可同时作 为 SIS(针 对 同 一 危 险 事件)的一部分来声明风险降低,除非在风险降低分析中考虑了共因失效 。
- 考虑了关于可被声明的风险降低的限制,报警系统设计和管理会用到这些限制,如访问安全规定 、变更管理和检查 、预防性维护和测试 。

IEC 61511-3:2016给出了可用来确定 SIS的 SIL的技术示例,也包含选择用于某个特定应用的方法时需考虑问题的指南 。

当确定是否需要风险降低时,需有过程安全和环境目标 。它们会根据特定的现场或运营公司而有所不同,并且可同未使用额外安全功能的风险等级进行比较 。在确定需要风险降低之后,有必要考虑需要执行什么样的功能以使过程返回到安全状态 。理论上,可以用 一 般用语描述这些功能而无需涉及某个特定技术 。 以超压保护为例,可把功能描述成防止压力上升超过某个规定值 。执行此功能的可能是泄压阀也可能是 SIS。 当如上描述功能时,则可在生命周期的下一 阶段(给保护层分配 SIF)来选择所使用的技术类型 。实际上,功能要求根据所选的系统类型是不同的;在某些情况下,此阶段和下 一 阶段可结合起来 。

总之,H&RA宜考虑:

a) 每个已确定的危险事件和导致该危险事件的事件序列;
b) 与每个危险事件相关联的事件序列的后果和可能性,可定量或定性表示;
c) 未提供进一 步指南;
d) 每个危险事件的必要的风险降低;
e) 为降低或消除危险和风险而采取的措施;
f) 在分析风险过程中所作的假设,包括估计的要求率和设备的失效率;宜详细说明操作约束或人为干预的置信度;

g) 未提供进一步指南；

h) 在每个 SIS生命周期阶段(如验证和确认活动)对安全相关系统有关关键信息的引用 。

H&RA 的信息和结果都宜文档化 。

随着采用的决策和可用信息更精确,可能有必要在整个SIS安全生命周期的不同阶段重复进行H&RA。还宜定期对 H&RA 进行再确认,并宜形成文档,以确保所做的假设与实际操作经验(见GB/T21109.1— 2022的 5.2.5.3)和当前功能安全管理计划(见 GB/T21109.1— 2022的 5.2.5.1)相匹配。

A.8.2.2 BPCS包括使过程及其相关设备按期望的方式运行所需的所有设备(见 GB/T 21109.1— 2022的 3.2.3) 。通常,BPCS设备不被认定符合 GB/T21109.1— 2022(见 GB/T21109.1— 2022中的 11.2.4),因此危险失效率不能假定为小于 10^{-5}每小时 。

在过程工业中,BPCS失效是 H&RA要考虑的重要原因(触发保护层动作的要求来源) 。 BPCS失效可能由正常运行 BPCS的任何要素造成,例如传感器、阀门、操作员失误或者逻辑解算器 。

GB/T 21109.1— 2022将 BPCS作为触发原因时的危险失效率限制为不低于10^{-5}每小时,除非BPCS按照 GB/T 21109的要求实施 。这种限制的理由是 ,GB/T 21109.1— 2022的功能安全管理系统及其规定措施和技术是降低系统性失效可能性至足够低水平的必要手段,以支持声明小于 10^{-5}每小时的危险失效率 。此限制保证了不满足 GB/T 21109.1— 2022要求的 BPCS不会有过高的置信度水平 。

A.8.2.3 未提供进一步指南 。

A.8.2.4 关于进一步指南,见 ISA TR 84.00.09:2013。

A.9 给保护层分配安全功能

A.9.1 目的

为了确定是否需要 SIF及其相关的安全完整性要求,考虑已计划(或已安装) 的保护层以及它们所提供的风险降低有多大很重要 。如果需要一个 SIS保护层,则宜确定该 SIS的每个 SIF的 SIL。

A.9.2 “分配过程要求”指南

A.9.2.1 本条的要求是确定要使用的保护层并将风险降低分配给 SIF。 实际上,只有在使用固有安全设计或其他技术系统存在问题时,才将安全功能仅分配给 SIS。

这类问题的例子包括对火炬能力的限制或者针对放热反应的保护 。使用仪表系统而不是像安全阀这类更传统方案的任何决定,都宜有坚实的理由来支持,而这种理由要经受得住制定规章制度的权威机构的质询 。

如上所述 ， H&RA与分配可能同时进行;在某些情况下,分配可以在 H&RA前进行 。 给保护层分配安全功能的决定通常根据经用户实践认为可行的依据做出 。还宜考虑行业良好实践 。然后在假定其他保护层是可信任的情况下,才决定是否用 SIS。例如,在已安装安全阀,并且它们是根据工业法规设计和安装的情况下,判定它们本身是否达到足够的风险降低 。在安全阀的大小和性能还不完全满足应用,或者禁止将气体释放到大气中的情况下,仅用 SIS限制压力 。

A.9.2.2 未提供进一步指南 。

A.9.2.3 在把一个安全功能分配给 SIS时,需考虑应用是低要求模式还是高要求/连续模式 。 过程领域中,在要求不是很频繁的情况下,安全功能通常在低要求操作模式下运行。 在这类情况中,GB/T 21109.1— 2022的表 4是常用的合适量值 。越来越多的应用在高要求模式中操作,在这种情况下,这类应用更适合作为连续模式,因为危险事件通常是在 SIS不能起作用时发生的 。在这种情况下，宜使用 GB/T 21109.1— 2022的表 5 中的合适量值 。失效立即导致危险的,在连续模式应用中是很少见的 。如果要求燃烧器或汽轮机速度控制功能平均失效频率低于 10^{-5}每小时才能满足特定危险事件频率,则可将上述功能规定为符合 GB/T 21109.1— 2022的连续模式应用 。

GB/T 21109. 1— 2022的表 4 中 SIL是通过 PFDavg来定义的 。 而目标 PFD_{avg}是通过要求的风险降低来确定的 。通过将没有 SIS时的过程风险与允许风险进行比较来确定要求的风险降低 。它可以通过 IEC 61511-3:2016所列技术按照定量或定性的原则来确定 。

GB/T 21109. 1— 2022的表 5用执行 SIF的危险失效平均频率来定义 SIL。SIL通过 SIS的可容许失效率并考虑特定应用中的失效后果来确定 。 当使用 GB/T 21109. 1— 2022的表 5 来确定要求的 SIL时，目标会基于 SIS的危险失效频率 。在使用 GB/T 21109. 1— 2022的表 5 时 ,使用检验测试间隔或要求率把危险失效频率转换成要求时的危险失效概率是不正确的 。尽管单位看起来是 一 样的 ,但会导致 GB/T 21109. 1— 2022的表 5 的不恰当转换 ,并可能导致不满足 SIL要求 。

要求时的平均失效概率目标或者危险失效频率目标适用于 SIF,并不适用于单个组件 、设备或 SIS子系统 。一个组件 、设备或 SIS子系统(如传感器 、逻辑解算器和最终元件)除了它与某个特定 SIF联系之外 ,不能给它指派一个 SIL。然而 ,组件可能具有一种系统性能力 ,这种能力是指 ,使用 一 些措施和技术来降低导致 SIS危险失效的系统性错误的可能性 。

H&RA和分配过程的输出 ,宜清晰描述保护层所执行安全功能 。对于 SIS,这 一 描述宜包括操作模式(即连续模式 、低要求模式或高要求模式)以及每个 SIF的 SIL要求 。它构成了 SIS安全要求规范的基础 。安全功能的描述宜明确说明要采取什么措施以确保功能和安全完整性要求得到理解 。

在此阶段 ,不必规定传感器和阀门架构细节 。决定采用什么样的架构比较复杂 ,特定系统是否要求 2oo3传感器和 1oo2阀取决于许多因素 。

A. 9. 2. 4 宜完全了解 GB/T 21109. 1— 2022 的表 4 和表 5 的含义。 特别是，单个 SIF 可以声明的 PFD_{avg}限制到 10^{-5} ,这相当于 10^{5} 倍的风险降低(SIL4) 。可靠性分析指出硬件随机失效的 PFD_{avg}小于 10^{-5}是可以实现的 ,但 GB/T 21109. 1— 2022的认为系统性失效和共模失效会限制实际可能达到的风险降低 。 强烈推荐在风险分析显示出需要高的风险降低的情况下，要注意到过程领域中 SIF要 达 到 SIL4是困难的 。宜考虑消除或降低源头的危险 、使用非 SIS的风险降低措施 、降低造成危险事件的可能性或者使用多个安全完整性较低的独立 SIF。在使用多个 SIF的情况下 ,宜考虑 SIF之间的相关性，包括同步进行检验测试的影响。 对这种影响进行考虑的方法是使用整体分析法对整体结构建模(见 IEC 61511-3:2016的附录 J) 。

A. 9. 2. 5 未提供进一 步指南 。

A. 9. 2. 6 为了达到较高的风险降低水平(如大于 10^{3}),可以使用多个 SIF。 当使用多个 SIF来达到较高的风险降低时 ,重要的是每个 SIF宜能独立地执行安全功能 ,并且各 SIF之间宜有足够的独立性 。

另外 ,在使用多个 SIF时 ,还宜考虑共因失效 。此外，还要满足 GB/T 21109. 1— 2022定义的所有其他要求 ,包括 GB/T 21109. 1— 2022的表 6 中定义的最低故障裕度要求 。

为了说明怎样组合所使用的多个 SIF来达到较高的风险降低水平 ,考虑下例：

由 2oo3变送器 、2oo3逻辑解算器和 1oo2最终元件构成的一个 SIF具有 PFD_{avg}为 3.05×10^{-4} 。该 SIF达到的风险降低大约为 3.3×10^{3} 。

使用两个这样的系统来产生一个 10×10^{6} ($3.3\times10^{3}\times3.3\times10^{3}$) 风险降低的假设是不正确的 。共因因素(如使用相同的技术 、根据同样的功能规范设计两个系统) 、人为因素(如编程 、安装 、维护)和外部因素(如腐蚀 、堵塞 、空气管道的冻凝 、闪电) 以及同步开展检验测试的相关性都将限制系统性能提高 。还有必要考虑两个系统间任何共用的部件 。

一种较可行的解决办法是使用尽可能多样性设备的 一个非冗余第二系统(为了最小化潜在的共因问题) 。然而 ,使用不同的组件可能会使维护更加困难 。 为每个应用程序选择最佳的解决方案 ,宜进行完全的分析 。

IEC 61511-3:2016的附录 J中给出了如何评价保护层之间的相关性和共因的进一 步指南 。

A. 9. 2. 7 关于如何评价保护层之间相关性和共同原因的影响，见 IEC 61511-3: 2016 的附录 J 中的指南 。

A. 9. 2. 8　未提供进一 步指南 。
A. 9. 2. 9　未提供进一 步指南 。

A. 9. 3　“基本过程控制系统作为保护层的要求” 指南

A. 9. 3. 1　在某些条件下 BPCS也可视为一个保护层 。

SIF不能在 BPCS中实现，除非 BPCS根据 GB/T 21109设计 。GB/T 21109. 1— 2022的 11. 2. 4声明: “如果不打算让 BPCS符合 GB/T 21109,则宜将 SIS设计成分开且独立的系统，以确保不影响 SIS安全完整性 。” 将 BPCS作为 SIS进行设计和管理需要应用 GB/T 21109中的生命周期要求 ,包括危险和风险分析、设计文档化、功能安全管理、变更的确认以及变更管理 。

风险降低只能分配给一个 BPCS保护层 ,除非满足 GB/T 21109. 1— 2022的 9. 3. 4 和 9. 3. 5 的要求，并且根据 GB/T 21109. 1— 2022进行进一 步的定量风险分析 。这一分析并非易事 ,它涉及到整个 BPCS设计的详细评估 ,包括硬件 、软件 、通信 、电源 、接口等 。这一分析至少宜考虑硬件的完整性 、为防止出现共因失效将保护层分开 、应用编程系统性错误管理 、硬件和软件的访问安全 、变更管理 、操作员交互 、配置控制和定期确认 。

在考虑一个 BPCS保护层时 ,宜对该 BPCS的设计和管理进行评估，以确保在与该 BPCS的整体风险降低要求比较时 ,该 BPCS保护层与触发源之间以及该 BPCS保护层与其他保护层之间共因失效 、共模失效 、系统性失效可能性足够低 。

A. 9. 3. 2　BPCS保护层声明的风险降低 ≤10时 ,不需要符合 GB/T 21109. 1— 2022。这使得 BPCS可用于降低风险 ,而无需按 GB/T 21109. 1— 2022的要求实现 BPCS保护层 。

宜通过考虑 BPCS的风险降低能力(由可靠性分析或以往使用数据确定)以及用于配置 、修改 、操作和维护的规程 ,宜对 BPCS保护层声明风险降低 ≤10进行判定 。

BPCS保护层宜以文件形式记录在功能规范中 ,描述为达到所分配的风险降低如何设计 、维护 、检验 、测试和操作 BPCS。

与 BPCS保护层设备相关的故障可通过过程运行 、自动化诊断 、机械完整性活动或触发另 一 危险事件(但不是用 BPCS降低风险的那个危险事件)来揭露 。故障检测宜使得 BPCS保护层采取规定动作来达到或保持安全状态 。例如 ,达到或保持安全状态所要求的规定动作(故障响应) 可包括该过程的安全切断(或依赖用于风险降低的故障 SIS子系统的过程部分)或确保在完成维修的同时安全运行的规定补偿措施 。要求故障响应动作在过程安全时间内完成 。

在给 BPCS保护层分配风险降低时 ,确保仍然提供访问安全和变更管理是非常重要的 。宜使用管理控制来控制 BPCS内保护层的访问和修改 。旁路某一 BPCS保护层(例如 ,使 BPCS功能处于手动模式)需要获得批准 ,且在旁路之前 ,补偿措施宜到位，以确保所要求的风险降低得以保持 。在做出可能会影响 BPCS保护层运行的变更之后 ,宜采取措施确认该保护层的功能性 。

A. 9. 3. 3　未提供进一 步指南 。

A. 9. 3. 4　对 BPCS保护层可以声明的风险降低 ,还会受到 BPCS保护层与其他保护层以及危险事件触发源之间独立程度的约束 。

整个 BPCS的详细分析宜证明该 BPCS中控制和保护设备是充分独立且分开的 ,这样才可以得出以下结论，即作为触发源的 BPCS失效引起该 BPCS保护层失效的概率足够低。 在这种情况下,认为 BPCS保护层是可信的，即使该 BPCS可能会触发危险事件 。

当 BPCS为触发源时,同一危险事件声明的 BPCS保护层不会多于一个,除非该 BPCS根据 GB/T 21109. 1— 2022设计和管理 。 图 A. 2说明了 BPCS保护层和 BPCS触发原因的独立性 。

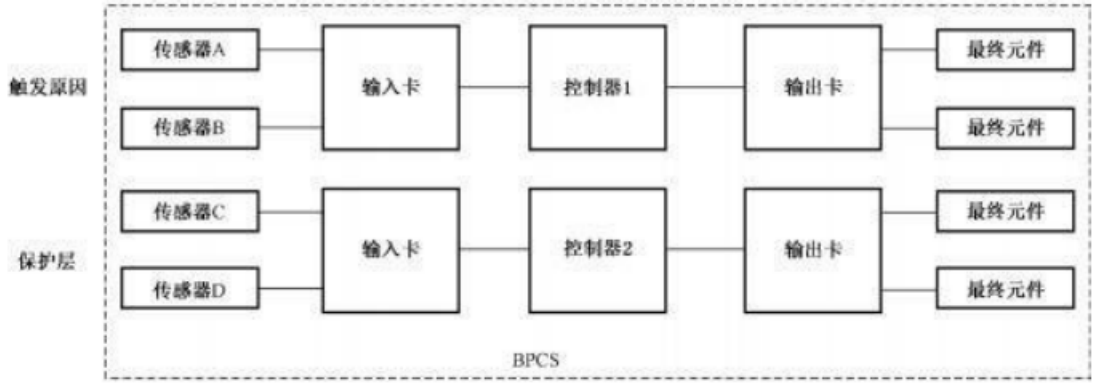


图 A. 2 BPCS保护层和 BPCS触发原因的独立性

例如 ,考虑一个流量控制回路是触发原因的情况 。此触发原因包括 一 个流量变送器 、一 个控制器 BPCS逻辑解算器和一个控制阀 。为了给 BPCS中的 一 个压力控制回路分配风险降低，压力变送器宜连接到一个独立的 BPCS逻辑解算器 ,该逻辑解算器调节一个独立的最终元件(例如到火炬系统的排气阀) 。保护层也可能是一个报警和操作员响应功能 。

在将 BPCS针对同一危险事件声明为触发源和保护层时 ,宜设计和管理整个 BPCS(包括图 A. 2 中说明的任何一个设备)使它满足所声明的平均失效频率 ,例如 $\leq 10^{-6}$/h(即当 BPCS作为触发源的时候，它的失效频率需 $\leq 10^{-5}$/h,作为保护层时它需要降低 10倍的风险 ,这样才能满足所声明的平均失效频 $\leq 10^{-6}$/h) 。这一声明宜通过 BPCS的定量分析来判定 ,其中定量分析考虑了含有 BPCS的设备之间出现共因失效和共模失效的可能性 。 由于随机失效和系统性失效造成的共同原因可能会限制 BPCS达到所声明的平均失效频率的能力 。

当触发源与 BPCS的失效无关时,同一危险事件声明的保护层可不多于两个,除非 BPCS根据 GB/T 21109. 1— 2022设计和管理 。下图 A. 3说明了给 BPCS分配的两个 BPCS保护层的独立性 。

A. 9. 3. 5 在声明将两个 BPCS保护层用于同一危险事件时 ,宜设计和管理整个 BPCS(包括图 A. 3 中说明的任何一个设备)使它满足所声明的降险能力 ,例如 ≤1/100(即当 BPCS作为保护层的时候 ,需降低 10倍的风险，因此两个 BPCS保护层需降低 100倍的风险，这样它所声明的降险能力才能 ≤1/100) 。GB/T 21109. 1— 2022的 9. 4. 1 和 9. 4. 2 中的条件和考虑适用于两个 BPCS保护层 。所声明的风险降低宜通过 BPCS的定量分析来判定 ,该定量分析考虑了含有 BPCS的装置之间出现共因失效和共模失效的可能性 。 由于随机失效和系统性失效造成的共同原因可能会限制 BPCS达到所声明的风险降低的能力 。

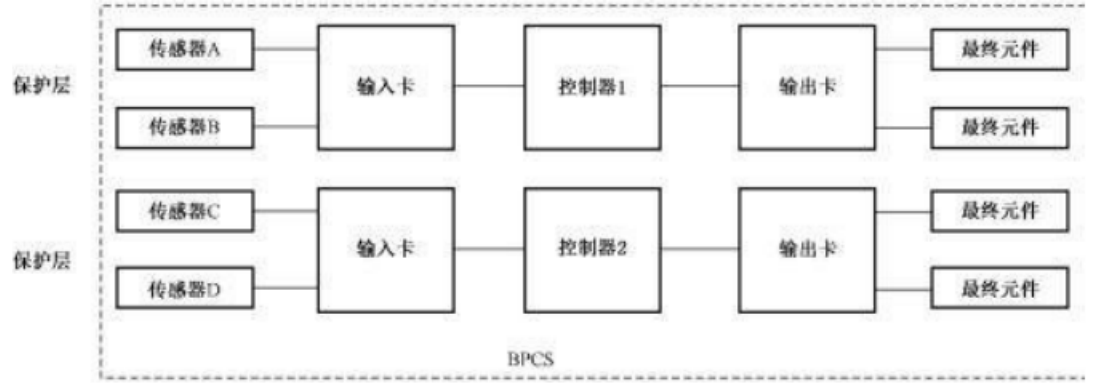


图 A. 3 分配给 BPCS的两个保护层的独立性

A. 9. 4 “防止共因失效、共模失效和相关失效的要求”指南

A. 9. 4. 1 在早期阶段宜考虑的一个重要问题是在每层中的各冗余部分之间(例如，同一压力容器上的两个安全阀之间)、各保护层之间或者各保护层和 BPCS之间是否存在任何共因失效。举例来说一个 BPCS测量的失效可能引起对 SIS提出一次要求，在该 SIS中使用了一个具有同样特性的设备。 在这种情况下,有必要确定是否存在使两台设备同时失效的可信的失效模式。在判明是一个共因失效的情况下,则可采取以下动作。

a) 可通过改变 SIS或者 BPCS的设计来减少共同原因。 降低共因失效的可能性的两种有效方法是设计的多样化和物理分离。这是通常优先选用的方法。

b) 当确定总的风险降低是否足够时宜考虑共同原因事件的可能性。这要求进行包括由要求原因以及保护系统失效构成的故障树分析。在这种故障树上可以显示出共因失效并通过适当的建模方法量化对整个风险的影响。

BPCS和 SIS共用的任何传感器或者执行机构都很可能引入共因失效。

A. 9. 4. 2 当对共因失效、共模失效和相关失效的可能性执行评估时,宜考虑下列因素。评估的范围、形式和深度取决于预期功能的 SIL等级。对安全完整性水平为 SIL3或者 SIL4的情况而言,共同原因、共同模式和相关失效的影响也许是决定性的。 以下是考虑的因素。

- 各保护层之间的独立性:宜进行失效模式影响分析，以确定单一事件是否能引起不止一个保护层失效或者 BPCS和一个保护层同时失效。分析的深度和严密性取决于风险。
- 各保护层之间的多样性：目标宜是各保护层和 BPCS之间的多样性,但并不一定总是能做到。使用从不同生产厂购买的设备也许能达到某些多样性,但如果使用同类型的连接方式把 SIS和 BPCS传感器连接到流程中,则多样性也许会受限。
- 不同保护层之间物理分离:物理分离可以降低由物理原因引起的共因失效的影响。 根据比如精确性和响应时间这样的功能需要,BPCS和 SIS的测量连接位置需有最大程度上的物理分离。

A. 10 安全要求规范(SRS)

A. 10. 1 目的

编制 SRS是整个 SIS安全生命周期中最重要的活动之一。通过这个规范,用户可定义怎样设计需要的 SIF和如何把这些功能集成到 SIS中。

使用此规范来执行 SIS的最终确认。

A. 10. 2 “一般要求”指南

SRS可以是单独一个文档,也可以是包含规程、图纸或公司标准惯例的几个文档的一个集合。 可由 H&RA小组和/或工程项目组拟订这些要求。

A. 10. 3 “SIS安全要求”指南

A. 10. 3. 1 如 GB/T 21109. 1— 2022所述,有若干宜在项目初期定义的设计要求以确保 SIF提供所要求的保护。

以下是有关 SRS的一些考虑。

a) 宜定义的首要条款是 SIF及其 SIL。 一个 SIF 的例子是“通过截断处于高压状态下的进口阀以防止反应釜超压”。典型的功能描述包含：

- 为了检测危险工况而宜监测的过程参数；

示例：检测压力上升超过某个规定值。 当压力处于某参数值时采取动作,该参数值需设定为超过正常操作范围且低于导致危险工况的某个值。需要为系统响应和测量精确度确定一个允许范围。 因此,在设置极值时,需要同负责设计和实施 SIS的人员进行讨论。

- 宜采取的行动，以及在什么时候采取措施防止危险事件发生 。 一 个简单的例子可能是在规定的时间内减少流到再沸器的蒸汽流量 。需注意的是，一般仅说明切断进入再沸 器 的蒸汽流量还是不够充分的 。设计人员需要知道什么对于成功运行是必要 的 。 例 如，根 据热负荷 ,在一分钟之内把流量降低到 10%以下就足够了 。在其他例子中 ,可能需要在几秒钟内紧密关断蒸汽流 。
- 不是为了防止危险事件而是可能有利于操作而采取的动作 。 这些动作可能包括报警 、上游或下游单元的关断，以减少对其他保护系统产生要求 ,或者消除危险起因后能快速起动的动作。值得注意的是,宜把这些非安全动作同防止危险工况的必要动作分开,以便把SIS的边界限定到必要范围内 。
- 识别出的需避免的会导致危险情况的过程状态或者 SIS操作顺序 。SIS的设计完成后 ,需要对风险进行进一 步分析，以考虑部分失效或 SIS误动作是否会产生新的危险或者成为已识别危险的附加诱因 。

b) 本规范宜定义每个已识别出的功能的过程安全状态 ,如哪个物料流的启/停 、哪个过程阀门的开/关以及任何旋转设备(泵 、压缩机和搅拌器)的运行状态 。如果将一个过程导向安全状态涉及顺序要求 ,则也要确定该顺序 。

在定义最终元件时 ,可考虑多样性的好处 ,例如 ,关断产品流及关断蒸汽流以降低高压 。

c) 在开始设计 SIS时 ,可定义所需检验测试间隔的要求，以便在设计中能把它考虑在内 。例如，如果要在计划的停车期间(如每三年)执行检验测试 ,则设计可能要求比检验测试间隔为 一 年时更高的冗余程度 。

可对以下方面进行考虑：

- 测试持续时间;
- 被测设备的状态(离线/在线)；
- 测试过程中的过程状态;
- 共因失效的检测;
- 错误(如测试完成后 SIS仍被屏蔽)的预防;
- 测试文档编制要求;
- 存档要求;
- 确保管理人员了解计划内容的需求;
- 确保相邻区域和其他受影响区域知晓即将进行测试的需求;
- 测试规程制定人员的技术资格和经验;
- 执行测试规程的人员的技术资格和经验 。

d) SIS的最长允许响应时间从过程达到跳闸条件开始 ，到最终元件达到安全状态为止的最后 一刻(防止危险发生) 。宜定义能手动使过程进入安全状态的要求 。例如 ,如果要求操作员能够从控制室或现场手动关闭一 台设备 ,则宜对此进行规定 。也宜规定 SIS逻辑解算器的手动停车开关的任何独立性要求 。

e) 宜规定在停车之后重新启动过程的所有要求 。例如 ,某些用户在主控面板上或在现场有电子复位开关 ,而另一些用户则可能使用带锁定手柄的电磁阀 。如果存在类似于这种复位动作的特殊要求 ,宜作为 SRS的组成部分 。

f) 如果存在误跳闸目标频率的要求 ,也宜作为 SRS的 一 部分进行规定 ,也是 SIS设计中的 一 个因素。

g) 宜详细说明 SIS和操作员之间的接 口 ,包括报警(预停车报警 、停车报警 、旁路报警和诊断报警)，图表和事件顺序记录 。

h) 也可能需要旁路以便能在过程运行的同时测试或维护 SIS。如果存在旁路这类设备的特殊要

求诸如键锁或口令,也宜把这些作为 SRS的一部分 。

i) 宜定义 SIS的失效模式和对检测到故障的响应 。例如，可以把变送器配置成失效导向跳闸或者失效远离跳闸状态 。如果把它设计成失效就远离跳闸状态,重要的是操作员能得到变送器失效的报警以及培训操作员采取的纠正动作。 关于对检测出故障的要求,可见 GB/T 21109. 1— 2022的 11. 3。

A. 10. 3. 2 未提供进一步指南 。

A. 10. 3. 3 本条涉及到应用编程安全要求指南 。 AP SRS确定了 PE AP功能的最低能力,还限制了会导致不安全工况的任何功能的形成 。 已经在 SIS要求中做出规定的 AP安全要求无需作为单独的 AP SRS进行重复说明 。

APSRS通常考虑了 SIS的系统架构 。该系统架构定义了主要的设备 、SIS子系统 、嵌入式软件和 AP,并确定了它们之间如何相互关联 、如何达到要求的属性(特别是安全完整性) 。嵌入式软件模块的例子包括操作系统 、数据库和通信 SIS子系统 。AP模块的例子包括在整个工厂内可反复调用的应用功能 。

AP架构也宜通过供应商所提供 SIS子系统的底层架构确定 。AP架构不得削弱硬件冗余,例如，如果处理器冗余(如 1oo1)低于传感器冗余(如 2oo3),则相关的 AP宜支持传感器所要求的表决(即 2oo3) 。

每个 SIF的详细功能安全要求通常利用逻辑图或因果图(见图 D. 2) 确定 。 在很多情况下,逻辑解算器供应商提供的编程语言可用于确定这些要求 。可以使用的典型语言有功能块图或因果矩阵 。在预计会使用模型检测技术时,还可使用诸如统一建模语言(UML)的专门格式,这些格式也是非常有用的 。所选用的由供应商提供的语言宜适用于该应用 。使用由供应商提供的语言来确定详细要求通常可以避免在将要求从其他文件编制形式翻译过来时出现错误 。可自由使用注释来定义安全和非安全功能以及所有安全功能的 SIL要求 。

在 BPCS中或者在与 SIF完全分离但能清楚链接到 SIF的应用程序部分中 ,宜在基本独立的 SIF功能行为(例如管理装置的开车和停车) 必需的要求范围之外实现 一 些附加要求 。此外 ,AP可包括实现整个 SIS架构的许多功能 、端到端诊断以及异常工况下的行为 。例如，与 SIF有关并结合了“失电跳闸”或“通电跳闸”原理的传感器(表决原则 :1oo2、2oo3等) 的架构定义了宜如何在 AP 中实现传感器表决 。确保没有任何一项附加功能的组合能超越基本应用安全功能是非常重要的 。

如果使用多个 SIS来实现单个 SIF,宜提供文件资料来解释每个 SIF 中需要实现哪些功能 。 如果使用多个 SIF来实现一个整体 SIF(例如组合两个较低 SIL的 SIF来达到更高的 SIL) ,则宜将每个 SIF的独立性和 SIF之间的相互作用记录在文档中 。 (见 F. 4 的系统架构和 IEC 61511-3:2016的附录 J) 。

注 1: APSRS确定了 PE AP功能的最低能力,还限制了任何会导致不安全工况的功能的开发 。

注 2: 已经在 SIS要求中做出规定的 AP安全要求无需进行重复说明 。

注 3: 该系统架构定义了嵌入式软件和 AP的主要设备和 SIS子系统,并确定了它们之间如何相互关联、如何达到要求的属性(特别是安全完整性) 。

注 4: AP架构可考虑供应商提供的 SIS子系统的底层架构。该 AP架构不能削弱硬件冗余— 例如,如果处理器冗余(如 1oo1)低于传感器冗余(如 2oo3),则相关的 AP宜支持传感器所要求的表决(即 2oo3) 。

注 5: SIS通常由三个架构化 SIS子系统构成 :传感器、逻辑解算器和最终元件。另外,SIS子系统可设有多个冗余设备，以达到要求的完整性等级 。

注 6: 设有冗余传感器的 SIS硬件架构可对 SIS逻辑解算器提出附加要求(例如 ,1oo2逻辑的实现) 。

宜处理引起 AP设计人员注意的 SRS中的任何冲突 、矛盾和遗漏 。AP 内 SIF的执行顺序所产生的影响也许是其中一个例子 。另 一个例子是 ,AP在涉及到能源中断时的响应 。

注 7: AP设计人员可以审核规范中的信息，以确保这些要求是清楚 、一致和可以理解的 。规定的安全要求中的任何缺陷均可被 SIS设计人员知晓 。

注 8: 随着 AP安全要求和可能的 AP架构变得越来越精确,可能会影响 SIS硬件架构(见下图 A. 4)，因此,SIS架构

开发人员 、SIS子系统供应商和 AP开发人员之间的紧密合作是必不可少的 。

图 A. 4 系统、SIS硬件和 SIS应用程序的关系

APSRS宜包括受保护过程所有操作模式中必需的全部功能 ,包括启动许可 、运行 、停车 ,还有 SIF的定期测试 。通常要求具备维护超驰能力 ,这样就可以在无需停止过程运行的情况下对传感器和最终元件进行测试 。需要涉及的因素包括 :

a) 实现用户 自定义 SIF必需的功能和时间要求 ;
b) AP系统与过程和人员的接 口 ;
c) 过程危险与 AP所提供功能之间的关系 ;
d) 为了保持在过程的安全范围内而允许的 AP行为界限(例如必须能处理错误的输入条件) ;
e) 逻辑解算器内提供的工具软件的允许功能(例如安全逻辑和 I/O优先于通信 、错误处理和逻辑解算器诊断) ;
f) AP运行的硬件平台和嵌入式软件 , 以及硬件和嵌入式软件的配置 ;
g) 由于系统功能问题(AP是其中的 一 部分) 可能导致过程出现危险(例如切断电源时出现的不适当的硬件失效模式) ;
h) 配套逻辑解算器的安全手册而对设计人员可以使用的方法和规程的限制 ;
i) 数据完整性和合理性检查 ,例如通信环节中的端到端检查 、传感器输入的范围检查 、数据参数的范围检查以及应用功能的多样化执行 ;
j) 对检测到的逻辑解算器硬件故障以及失效数据完整性和合理性检查的检测准则和响应 。
k) 为了避免在开发过程的后期出现困难 ,考虑用于表明 AP要求已达到的策略也是非常重要的 。

A. 10. 3. 4 使用 FPL设备时(例如智能传感器 、智能变送器 、HMI图形面板) ,可将设备配置的要求作为SRS的一部分进行规定 。

A. 10. 3. 5 B. 1、F. 17、F. 20和 G. 2 给出了实现 GB/T 21109. 1— 2022的 10. 3. 2. 3 以及 AP安全要求的附加指南 。上述附加指南会因为范围的广度 、AP语言和过程应用 、复杂程度而有所不同 , 以说明满足 AP安全要求有多种可能性 。

A. 10. 3. 6 关于如何构建 AP安全要求的例子 ,见 B. 4. 3. 2 和附录 F 中的步骤 F. 3。

A. 11 SIS设计和工程

A. 11. 1 目的

本章的目的是提供SIS的设计指南。每个SIF都有它自己的SIL。SIS的某个设备,如逻辑解算器,可以被不同SIL的若干个SIF使用。

A. 11. 2 “一般要求”指南

A. 11. 2. 1 未提供进一步指南。

A. 11. 2. 2 关于AP指南,见A. 12. 2. 4。

A. 11. 2. 3 如果SIS中的AP要实现不同SIL的SIF,则宜有明确标记。这可以使每个SIF的AP追溯到正确的传感器和最终元件冗余,也可以使多个功能的功能测试和确认测试与SIL是相匹配的。标记要体现出SIF和SIL。

A. 11. 2. 4 有时,SIS设备会由于操作原因而被BPCS使用。GB/T 21109. 1— 2022的第11章有若干SIS设计要求。其中一项是SIS和BPCS之间的独立性。

由于以下原因,SIS通常同BPCS分开。

a) 减少共因失效、共模失效和系统性失效,从而将BPCS失效对SIS的影响降至最低。

注 1: SIS与BPCS分开符合保护层的概念。当BPCS失效时,单独的SIS是一个独立的保护层。

b) 保持与BPCS有关的变更、维护、测试和文档编制的灵活性。

注 2: 通常SIS比BPCS有更高的健壮性要求,而且不会要求BPCS具有和SIS一样的健壮性要求。但需注意,不受控的BPCS修改可能对SIS要求增多。

注 3: SIS与BPCS分开可以使通常由不同操作人员进行的各个系统的维护分开。

注 4: 如果BPCS与SIS组合在一起,则为了满足SIS的变更管理和配置管理要求,可限制对BPCS编程或配置功能的访问。

注 5: 在对BPCS与SIS共用的任何设备进行变更之后,可提供一些手段来确认SIS。

c) 有助于SIS设备的识别和管理,从而使SIS的确认和FSA更直观和清晰。

d) 支持SIS的访问安全并增强SIS的网络安全,这样对BPCS功能或数据进行修改时不会影响SIS。

注 6: 共用接口和设备可作为SIS组件和设备进行管理,除非硬件和软件配置提供了功能分离。

注 7: 可特别考虑写入的限制条件,防止对SIS的未授权写入或意外写入。

e) 减少为确保对SIS和BPCS适当设计、验证和管理而需要开展的分析。

注 8: 在共用设备的失效可对SIS产生要求的情况下,可进行分析,以确保失效的整体平均频率满足预期值。这一分析可涵盖所有的BPCS和SIS设备,如传感器、逻辑解算器、最终元件、数据通信、公用设施、操作员站以及工程师站。

如果BPCS与SIS共用设备,则宜进行进一步分析,以证明BPCS设备的设计和管理:

- 达到BPCS功能和SIF的功能要求;

注 9: SIS之外任何硬件或软件的失效不能妨碍任何SIF的正确运行。

- 满足达到组合系统失效目标平均频率必需的完整性要求;

注 10: BPCS设备的失效不能成为危险事件的触发原因或导致SIF(针对当前评估的特定事件)危险失效(或无效/旁路),除非某一冗余设备能触发SIS动作。可进行分析以评价BPCS和SIS设备共用的影响。

注 11: 可对共模失效、共因失效或相关失效(如引压管堵塞、包括旁路在内的维修活动、不正确操作的管线隔离阀等)的概率进行充分评估并确定其足够低。

- 根据GB/T 21109. 1— 2022进行管理,包括检验测试、访问安全和变更管理。

SIS和BPCS之间的分离可使用同型分离或异型分离。同型分离意味着BPCS和SIS使用相同的技术,而异型分离则意味着使用同一制造商或不同制造商的不同技术。

与有助于降低随机失效的同型分离相比，异型分离还有利于降低系统性故障概率(同时和/或由于同一原因影响多个通道)，从而减少了多个通道的相关失效 。

在 SIS和 BPCS之间的同型分离在设计和维护时有一些优势，因为它降低了维护错误的可能性，特别是选择在用户组织范围内此前还未使用过的各种设备 。

虽然要考虑共因失效的源头和影响，并且要降低它们的可能性，但对 SIL1和 SIL2而言，SIS和 BPCS之间的同型分离是可接受的 。共因失效的一些例子是：

- 仪表连接和引压管的堵塞；
- 侵蚀和腐蚀；
- 由于环境引起的硬件故障；
- 软件错误；
- 供电和电源 。

注 12: 公用设施(例如供电)可采用传统的可靠性方法分析 。β 因子的使用与本实例无关 。

- 人为错误 。

一般可供 SIS和 BPCS分离的区域有 4个：

- 现场传感器；
- 最终元件；
- 逻辑解算器；
- 配线 。

BPCS和 SIS之间也不一定需要物理分离，其条件是它们之间宜保持独立性，并且设备布置方式和所使用的规程可以保证 SIS不受下列因素的危险影响：

- BPCS的失效；
- 在 BPCS上进行的作业，如维护 、操作或修改 。

若需要规程来确保 SIS不受危险影响，SIS设计人员宜规定要使用的规程 。

a) 现场传感器

BPCS和 SIS共用单个传感器时要求进一 步地审查和分析 。 因为此单 一 传感器失效可能产生危险情况，故有必要进行额外的审查和分析 。

注 13: 例如，BPCS和 SIS高液位跳闸使用同一个液位传感器，如传感器发生失效置低位(即低于液位控制器的设定值)，可能对高液位跳闸产生要求 。传感器失效置低位导致控制器打开阀门，由于 SIS也使用该传感器，而它并不会检测到产生的高液位工况 。

在 BPCS和 SIS功能共用单一传感器的情况下，一般只有在传感器诊断可把危险失效率降到足够低且 SIS能在要求的时间内把过程置于某个安全状态时，才能满足 GB/T 21109. 1— 2022的要求。

共用传感器(例如变送器 、分析仪和开关)宜由 SIS供电 。还宜考虑在共用设备由于检出故障 、维修或测试而停止运行的时段内需要实施的补偿措施 。对于较高的 SIL,通常需要使用同型或异型冗余的单独的 SIS传感器来满足要求的安全完整性 。

在使用一个单独 SIS传感器时，通过隔离器或保证 BPCS失效不会导致 SIS产生危险失效的手段来将信号复制到 BPCS是有益的 。通过 BPCS与 SIS传感器之间进行信号比较，可提高诊断覆盖率 。

当使用冗余 SIS传感器时，通过隔离器或保证 BPCS失效不会导致 SIS产生危险失效的手段也可把这些传感器连接到 BPCS上 。BPCS 中的适当算法(如“三取中”)可以通过降低 SIS的要求率来提高安全性 。

对 SIL2、SIL3或 SIL4的 SIF来说，通常需要使用具有同型或异型冗余的单独的 SIS传感器来满足硬件故障裕度要求和要求的安全完整性 。

b) 最终元件

与共用传感器的情况类似，BPCS和 SIS共用单个最终元件时，也需要进行进 一 步的审查和分析，因为此单一最终元件的失效可能会产生危险情况 。

注 14: 例如，BPCS和 SIS共用一个阀门时，如果阀门失效于打开位置，则可能产生要求，出现这一要求时，如果阀门不能按要求关闭，则会导致 SIS出现危险失效 。

在 BPCS和 SIS共用一个最终元件的情况下，一般仅当最终元件诊断可把危险失效率降到足够低，且 SIS能在要求的时间内把过程置于某个安全状态时，才能满足 GB/T 21109. 1— 2022 的要求 。

实际上，对于 SIL1应用而言要达到把危险失效率降到足够低也是很困难的，即使共用最终元件设计保证 SIS动作超驰 BPCS动作 。还宜考虑在共用设备由于检出故障 、维护或测试而停止运行的时段内需要实施的补偿措施 。对于 SIL2、SIL3或 SIL4的 SIF,通常需要使用具有同型或异型冗余的单独 SIS最终元件来满足要求的安全完整性 。例如，对于气动阀来说，把 SIS直接连接到从执行机构(例如位于阀门定位器与执行机构之间)排出空气的电磁控制阀上，可以实现 SIS动作超驰 BPCS这一 目标 。对于电动阀来说，可将接线设计成 SIS将控制阀置于并保持安全状态，直至复位 。

当使用冗余最终元件时，这些最终元件可同时连接到 SIS和 BPCS上 。

即使使用冗余最终元件，也需考虑 BPCS与 SIS之间的共因失效 。

交错测试冗余阀门，并执行相关规程，可降低共因失效的影响 。

当最终元件为阀门时，还需考虑：

- 阀门设计宜保证 BPCS失效不会导致 SIS无法使用共用阀门动作；
- 阀门设计在功能上使 SIS和 BPCS使用兼容；

注 15: 这可能是困难的，因为一些 BPCS阀门都安装为“流开”，一些 SIS阀门都安装为“流闭”。对于 SIS阀门来说，执行机构的功率要求可能不同于控制阀的功率要求 。

- 切断要求 。

注 16: 当通过控制阀的过程泄漏率不影响 SIF执行规定功能和防止危险时，该泄漏率是可容忍的 。

- 共用最终元件设计宜确保 SIS动作超驰 BPCS动作；
- 类似过程应用中阀门可靠性的经验；
- 阀门的不安全失效模式；
- 确保 SIS完整性的操作规程；

注 17: 例如，旁通阀可能会被锁定在关闭位置，并且会受到管理规程的影响，同样，回流线的弹簧关闭阀(例如液压)可能会被锁定在打开位置 。

- 检验测试要求 。

注 18: 可考虑部分行程测试或在线测试要求，并考虑它如何影响操作 。

c) 逻辑解算器

通过 BPCS和 SIS逻辑解算器实现分离和独立的能力因应用中使用的技术(即电气 、电子和可编程电子)而异 。

- 电气

  很多以往过程和一些现有过程采用含气动技术的 BPCS以及含电气技术的 SIS。 利用这些技术，可以很容易地在这种应用类型中实现分离和独立性，因为它们要求使用不同的外壳 、不同的物理布局和硬接线 。

- 电子

  很多以往过程和一些现有过程采用了电子技术不具有嵌入式可编程电子性能的 BPCS以及含电气技术的 SIS。利用这些技术，可以很容易地在这种应用类型中实现分离和独立性 。使用无嵌入式可编程电子技术的电子 SIS也是一种可行的手段 。

- 可编程电子(PE)

一些应用将 PE技术用于它们的 BPCS,并将电气技术用于它们的 SIS。 这些配置是固有分离和独立的，因为很多通信直接通过线连接,集成物理装备不具备优势 。

目前 ,过程领域中首选的 BPCS/SIS技术装备是将 PE技术同时用于 BPCS和 SIS。这 一 配置提供了最大的灵活性 ，因为它具有远程改变 BPCS和 SIS中 AP的能力以及在 BPCS与 SIS之间互换信息的能力 。不幸的是 ,在试图维持 BPCS与 SIS之间的分离和独立性时 ,这些特性可能会适得其反 ,除非在安全生命周期的设计阶段进行适当的分析 ,并证明功能独立性(例如通过不同的技术) 。

SRS(GB/T 21109. 1— 2022第 10章)宜提供如何使用 BPCS和 SIS技术装备达到分离和独立性的指南 。 由于引入了很多为 BPCS和 SIS提供额外安全性的新工具 ,也已经受到额外的帮助 。关于在 SIS与 BPCS之间提供不同分离和独立水平的实用 BPCS/SIS控制系统配置和安全工具 ,见 ISA TR 84. 00. 09:2013。

一些 PE逻辑供应商为控制器提供封装在同 一 物理外壳中的 BPCS和 SIS。在使用这 一 方法之前 ,应先仔细分析逻辑解算器的安全手册以及 ,并仔细分析置于 BPCS和 SIS的操作和维护中的要求如何遵守该设施的过程安全管理标准和 SRS。

d) 配线

有关给跳闸系统供电的问题 ,通常 BPCS和有关现场设备的配线是同 SIS和它的现场设备的配线分开的 ,这是因为安全功能可能意外失效而不通知跳闸系统 。有关这类系统的典型指南包括了安装 SIS和 BPCS专用的多芯电缆和接线盒 。 在配线未分开的情况下，为了减少维护中可能产生的误差所导致的 SIS失效 ,宜使用良好的标号和维护规程 。

注 19: 给跳闸系统供电涉及到 SIF电路 ,在正常工作状态下 ,该电路的输出和设备处于断电状态下 。施加动力(如电 、气体)就产生一 次跳闸动作 。

加电跳闸系统和断电跳闸系统的电缆支持系统(如电缆支架、管道),除另有原因(如电磁干扰)要求分开外 ,可以共用 。关于给跳闸系统供电的问题 ,宜附加对火灾风险区电缆支架防火的考虑 。

A. 11. 2. 5 在安全工厂运转中 ,操作员 、维护人员 、调查员和经理都有 自 己的任务 。 不过正如仪表和设备可能出现功能失常或失效一样 ,人也可能犯错误或者不能执行某个任务 。

因此 ,人的表现也是系统设计和完整性因素 。在把 SIS的状况通知给操作和维护人员的过程中 ,人机接口(HMI)尤为重要 。

人的可靠性分析(HRA)宜标明引起人犯错误的条件 ,并根据以前的统计和行为研究提供估计的误差率 。作为化工过程风险组成部分的人为误差的例子包括：

- 设计中未检测到的误差；
- 操作中的误差(如误差的设定值)；
- 维护不当(例如用一个失效动作不正确的阀门来替换另一个阀门)；
- 校准 、测试或解释控制系统输出时的误差；
- 不能正确响应一次紧急事件 。

注 ：附加指南见以下参考：

- CCPS/AIChE过程工业中提高绩效的人因方法(第 1 版) ,JohnWiley& Sons(2007) ,ISBN 0 470117540;
- CCPS/AIChE过程安全中防止人为错误的指南(第 1 版) ,JohnWiley& Sons(2004) ,ISBN 0816904618;
- CCPS/AIChE化学过程定量风险分析(第 2 版) ,纽约 :美国化学工程师协会(2000) ,0 81690720X;
- HSE减少错误和影响行为 ，HSG48,卫生与安全管理局 ,伦敦(2009) ,ISBN 9780 717624522;
- ISA TR 84. 00. 04:2015第 1部分 ，附录 B,ANSI/ISA-84. 00. 01-2004指南(IEC 61511) 。

A. 11. 2. 6 未提供进一步指南。

A. 11. 2. 7 本条论述了如果在纠正跳闸工况后,SIS立即自动重新起动该过程时可能产生的危险。宜分析每个 SIF, 以便确定一旦纠正了跳闸工况宜怎样复原该 SIF。一般只有在操作员的手动动作之后,才可能重新起动。

在图 F. 11的第 4 页第 1行中,说明了将某一功能置于安全状态时,该过程仍然处于安全状态的功能示例以供指南。

A. 11. 2. 8 手动意味着 SIS逻辑解算器和 BPCS控制系统二者是独立的,配备它们是为了在发生一次紧急事件时操作员能够启动停车。为了满足安全功能完整性要求,可考虑 SIS最终元件的手动操作方式,但应适当考虑相关的人为因素和共因失效。在 SRS中通常定义有手动停车的要求。

在某些情况下,手动关机可能会给设施带来额外的风险(例如在要求按顺序关机的情况下);在这种情况下,手动关机可能是 SIS提供分段关机的一次输入。

倘若必要并且危险和风险评估小组认为合适,就可把紧急停车连接到 SISPE逻辑解算器(例如当要求按顺序停车时)。

A. 11. 2. 9 本条指出需要分析SIS和其他保护层之间,而不仅仅是SIS和BPCS之间的独立性(见GB/T 21109. 1— 2022的图 9)。

在 SIS与其他保护层之间交错进行检验测试,可以降低同时发生失效的概率。

在有些情况下,BPCS和 SIS之间不完全分离是可以接受的,尤其是在共用设备的一次失效不会引起对 SIS提出一次要求的情况,在这种情况下需按照 GB/T 21109. 1— 2022实现共用或共享设备。

在 BPCS和 SIS二者使用同一设备类型的情况下,如果共用设备的共因失效可引起危险事件并导致向 SIS提出一次要求,则宜进行一次分析,以确保失效的整体平均频率满足预期值,从而确定与共用设备的危险失效相关的危险。

GB/T 21109. 1— 2022还指出,确保 SIS与其他系统之间的设计保持必要的独立性,即设计到 SIS中的非安全独立性,不会遭到 BPCS的破坏。例如,如果为了在 BPCS或其他非 SIS设备及工具中使用而生成的应用数据用于 SIS的设计,则有可能会使共同失效模式在这两个系统之间蔓延。另一个例子是允许 BPCS的超驰可以在系统中实现而无需将“许可”开关从 BPCS中分离出来的 AP。在应用数据被“泄漏”到另一系统和起动超驰的情况下,会从“镜面反射”中产生其他例子。

A. 11. 2. 10 提供 BPCS和 SIS二者所使用的一个共用器件的注意指南。GB/T 21109. 1— 2022的 11. 2. 10注中的“足够低”意味着由其他保护层(不是 SIF)的失效率组合成的共享设备的危险失效率仍满足共同风险准则。

A. 11. 2. 11 在失去动力源的最终元件失效后不能进入安全状态(例如,给跳闸系统供电)的情况下,宜考虑包含本地手动方式达到安全状态的条款。

A. 11. 2. 12 未提供进一步指南。

A. 11. 2. 13 安全手册的目的是用文件记录如何才能安全应用某设备、SIS子系统或系统的所有相关必要信息。

注 1: 该安全手册计划涵盖制造商和终端用户的信息,可酌情分成多个部分,例如硬件、固件和 AP。

注 2: 关于 IEC 61508的符合性项目,制造商的输入为符合 GB/T 20438. 2— 2017的附录 D要求的安全手册。

该安全手册宜包括但不限于以下信息:

a) 项目及其拓扑图(示意图)的简要描述,包括硬件和软件;

注 3: 根据 GB/T 21109. 1— 2022的 11. 4. 4进行的任何硬件故障裕度减少或增加,可在该安全手册中判定。

b) 与 AP有关的修订和约束条件识别;

注 4: 关于应用编程相关信息的更多细节,可查看 GB/T 21109. 1— 2022的第 12章。

c) 硬件和固件修订本的识别;

d) 操作描述,包括安全状态的定义以及失效安全操作;

注 5: 可考虑不同的操作模式,如启动 、正常操作 、降级操作和要求模式 。

e) 关于操作 、维护和测试的所有假设清单;

注 6: 这些假设可包括使用条件 、预防性维修 、如何进行检验测试以及诊断故障的跟踪 。

f) 与项目安全功能有关的所有限制和约束条件清单;

注 7: 限制和约束条件包括但不限于配置设定 、环境和过程限制条件 。

g) 设备的失效模式和对应的失效率;

注 8: 失效率可来源于制造商,也可来源于现场经验 。

h) 可靠性分析需要的其他参数,如有效寿命 、维修时间 、共因失效率(如果适用);

i) 检测出故障和警告的响应或相应行为;

j) 制造商的操作和维护说明以及检验测试间隔建议(如适用);

k) 为了避免和控制系统失效而采取的措施,包括软件失效和共因失效(如适用);

l) 如何通过定期功能测试和诊断来发现每种失效模式的信息,包括诊断测试间隔;

m) 该安全手册需包括关于设备使用的限制条件,其中含有与它的配置相关的细节 、接口 、安装 、诊断 、平均维修时间 、故障响应 、测试间隔和 AP语言限制条件 。

A. 11. 2. 14 未提供进一 步指南 。

A. 11. 3 “检测到故障时的系统行为要求”指南

A. 11. 3. 1 未提供进一 步指南 。

A. 11. 3. 2 未提供进一 步指南 。

A. 11. 4 “硬件故障裕度”指南

A. 11. 4. 1 安全系统的传统设计方法是保证任何单 一 故障不会造成预定功能丧失 。具有故障裕度为 1 的系统结构,如 1oo2或 2oo3, 即使存在 一 个危险故障,在要求时它们仍能起作用 。这些系统过去用作安全系统的一种标准方案,可保证它们足够健壮能承受硬件随机失效 。故障裕度结构还为宽范围的系统故障(主要是硬件中的系统故障)提供保护,因为这类故障不一定在同一 时刻出现 。

GB/T 21109. 1— 2022认识到过程工业中安全系统的性能不只需要一级,因此GB/T 21109. 1— 2022已采用了安全完整性等级的概念,此概念包含了系统性能的提高与特定危险事件所需的风险降低有关 。 因为有不同的性能级,因此各个性能级不再适合预期所有的安全完整性等级都是故障允许的 。但在选择适用于某个特殊完整性等级的结构时,重要的是要保证这种结构对于硬件随机失效和系统失效都足够健壮 。为了保证对随机硬件故障的健壮性,GB/T 21109. 1— 2022要求执行一次可靠性分析 。

本文件要求瞄准的目标是保证结构具有随机硬件故障和某些系统故障所需的故障裕度 。在决定所需的故障裕度值时,宜考虑以下系列因素:

a) 在 SIS或 SIS子系统中使用的设备的复杂程度;

b) 在设备的选择 、安装和配置以及确定其操作和维护规程的过程中,如果已经了解并考虑了设备故障的性质,则该设备不大可能会在操作过程中受到系统故障的影响;

c) 来自现场经验的失效数据;

d) 所涉及应用的安全完整性水平要求;

e) 故障能导致某个安全工况或能被诊断所检测,从而能采取某个规定动作的量值;

f) 由于安全失效造成的误动作(当故障裕度增加时,误动作通常会增多,反过来,误动作增多会产生新的危险或者是现有危险的一个附加原因,在误失效目标频率方面,也会变得不可接受);

g) 可大幅减少根据故障裕度所预期好处的共因失效和系统失效;

h) 当危险失效的恢复耗时过长时,故障裕度有可能真正达到降低至零(例如,其故障不在短于 0. 8 倍MTTF内纠正的 2oo3结构会比 1oo1结构更差);

i) 对于所有功能来说可能都不切实际的冗余可行性；

j) 涉及 SIS(或其子系统)的各种 SIF。

注 1: 在低要求或高要求下,可能会要求运行 SIS子系统,这由运行模式决定。可规定某一SIF选择一个阀门来响应规定的过程偏差。无论是在手动复位模式还是在自动复位模式中,SIS都将阀门维持在安全状态,直至执行其他动作指令。SIS中响应危险事件操作的硬件故障裕度要求可根据低要求模式确定,其在关机状态下的其操作规则根据高要求模式确定。

注 2: 已经确定了最低硬件故障裕度,以便缓解 SIF设计中的潜在缺点(可能是由于在 SIF设计的过程中由于做出多个假设而形成的),同时降低各个过程应用中所用设备失效率的不确定度。

A. 11. 4. 2 为了应用硬件故障裕度要求,需要很好地理解 SIS子系统的概念(见 GB/T 21109. 1— 2022的3.2.7.8)。

硬件故障裕度的要求适用于整个 SIS或需要执行 SIF的 SIS子系统,不适用于子系统内的单个器件。例如,在某一传感器 SIS子系统含有许多冗余传感器的情况下,故障裕度要求适用于传感器 SIS子系统整体,但不适用于单个的传感器。

A. 11. 4. 3 IEC 61508考虑了上文 11. 4. 1 中所述的因素,并采用两条不同的路径(称为 1_H 和 2_H)规定了 GB/T 20438. 2— 2017中要求的故障裕度范围。在为过程领域编制这一特定领域的标准时,认为路径 2_H 更适用于过程领域。 因此,GB/T 21109. 1— 2022中的故障裕度要求以 GB/T 20438. 2— 2017中的路径 2_H 为基础。GB/T 20438. 2— 2017中的路径 1_H 可作为替代途径应用。 宜注意,与 GB/T 21109. 1— 2022的表 6 中所述的内容相比,为了满足过程可用性要求(例如假失效频率目标),SIS子系统设计可能需要更多设备冗余。

用于 IEC61511符合性的途径 1_H 评估宜考虑预期操作环境。对现场设备来说,运行环境通常会对已证实的故障率产生重大的影响,它也可能影响安全失效和危险失效的分布。

A. 11. 4. 4 故障裕度可通过非同型冗余设备提供(例如,当多样化冗余实现时)。 实际上,SIS的硬件故障裕度由导致该 SIS中总的危险失效的独立设备失效的最小组合给出。如果已经将 SIS分成多个独立的 SIS子系统,则它的硬件故障裕度等于其 SIS子系统硬件故障裕度的最小值。

对 SIS进行在线维修期间,可放宽硬件故障裕度要求。不过,宜对与任何放宽有关的关键参数预先进行评价(例如,将 MTTR或测试持续时间与维修或测试期间出现过程要求的概率相比)。 这需要包括在于 SIL声明有关的概率量值计算(PFD_{avg}、PFH)中。

根据所选用的架构,降低硬件故障裕度可能会导致危险事件中的风险提高。宜评估持续带已知故障运行的风险,以确定是否需要采取补偿措施。

当某些单一失效/故障由于设计和构建所特有的特性而具有非常低的概率时,可将它们排除在外(见 GB/T 21109. 1— 2022中 3. 2),即对声明进行故障排除的串行设备危险失效之和的目标失效措施的贡献值不得超过1%。宜对任何此类失效/故障排除进行判定和文档记录。然后,通常无需考虑限制(依据硬件故障裕度)含有那些单一失效/故障的任何 SIF的安全完整性。

注 1: 在现场布线的情况下,常常会假定现场装置数据包括现场设备到终端设备的现场布线,因为现场布线的未检出危险失效率比现场设备低得多。一般而言,只有当硬件故障裕度需要用于现场设备时,才会为布线提供硬件故障裕度。在使用其他信号通信形式时,由于运行环境中的未检出危险失效率较高,因此可能需要单独确定信号传输设备的硬件故障裕度。对这些形式的通信来说,与现场设备比,信号通信设备可能会要求更高的硬件故障裕度。

注 2: 在这一分析中,通常不考虑执行独特功能(SIS通常不要求成功运行,且不大可能会影响 SIS根据要求操作的能力的功能,例如操作员接口、工程站、维护管理系统和数据记录器)的系统设备。

注 3: 当可以将某些故障排除在外时(根据上述准则),可能会降低最小 HFT(见 GB/T 21109. 1— 2022的11. 4. 6)。

A. 11. 4. 5 GB/T 21109. 1— 2022的表 6 定义了 SIS或 SIS子系统的最低故障裕度。故障裕度要求由 SIS所实现 SIF的所需 SIL确定。在建立硬件故障裕度时,以下假设是可以接受的,即已经为该应用选择了恰当的 SIS或 SIS子系统,并且子系统的安装、试运行和维护都准确无误以至可以在评估中将早期

失效和老化相关失效排除在外 。在确定硬件故障裕度时 ,可将人为因素排除在外 。

A. 11. 4. 6 故障裕度是获得某一强健架构已经达到的所需可信度的首选方案 。 当 GB/T 21109. 1— 2022的 11. 4. 6 适用时 ,该判定的目的是证明硬件故障裕度降低的拟用替代架构将提供等效或更好的解决方案(例如使用其他可验证手段如认证或类似手段) 。宜提供以下方面的证据 :

a) 与 GB/T 21109. 1— 2022的 11. 4. 5 中规定的硬件故障裕度要求的符合性也许会引入导致整体安全性下降的附加失效 ;

b) 如果硬件故障裕度降至零 ,则可将执行 SIF的 SIS中识别的失效模式排除在外 , 因为与所考虑SIF的目标失效量相比 , 已识别失效模式的危险失效率非常低 。

注 1: 实现较低硬件故障裕度的例子包括 :备份设备[例如 ,解析冗余(通过其他传感器输出的物理计算结果 ,更换已失效的传感器输出)] ;使用含有相同技术的更可靠项目(如果可用) ;变成更可靠的技术 ;通过使用不同的技术来降低共因失效的影响 ;增加设计余量 ;约束环境条件(例如电子元件的环境条件) ;通过收集更多的现场反馈或专家判定来降低可靠性不确定度等 。

注 2: 只有当检测和修理其他冗余零件失效之前的某一零件的失效概率较高时 ,硬件故障裕度才是有效的 。在维修非常困难(如果不是完全不可能维修)的情况 下 , 当 处 理 位 于 远 程 或 不 利 位 置(例 如 海 底 SIS) 中 的 系 统 时 , 硬件故障裕度的好处会降低 ,在这些情形中 ,SIS的设计可以为失效鲁棒性设计 , 即依赖固有的元件可靠性而不是硬件故障裕度 。

注 3: 如果由于故障裕度原因安装了附加工业组合全电压电机起动器(即设有控制变压器和指示继电器的组合保险开关和接触器 ,还设有用于连接和断开三相可逆或不可逆电动机电源的过载和短路保护设备) ,则可能会降低总的过程安全 。这是因为在采用多个电机起动器时相较于单个电机起动器时会增加元件的数量 ,从而导致 :

- 假跳闸 ;
- 设计更复杂(例如过载和短路保护协调) ,并在获取关于冗余电机起动器行为和失效模式的完整知识时出现更多困难 ;
- 维护 、检验和测试 ;
- 暴露于高压 ;
- 相间故障 , 由于多个组合满压电机起动器之间缺乏同步性(通常由布线错误造成)造成 ;
- 暴露于电弧 ;
- 需要重启 。

使用单一 工业组合满压电机起动器而不是冗余的进一 步判定通过以下考虑提供 :

- 很好地定义了所有元件的失效模式 ;
- 可以确定故障条件下电机起动器的行为 ;
- 工业手动起动器或工业组合满压电机起动器不依赖于软件执行它们的规定功能 ;
- 有足够的可信任数据显示 ,用于检出和未检出危险失效的声明失效可以量化随机硬件失效 ;
- 工业组合满压电机起动器的 MTTFdu值较低 ;
- 对使用定量程序核实是否使用了工业组合满压电机起动器进行判定 。

A. 11. 4. 7 未提供进一 步指南 。

A. 11. 4. 8 未提供进一 步指南 。

A. 11. 4. 9 未提供进一 步指南 。

A. 11. 5 “设备选择的要求”指南

A. 11. 5. 1 目的

未提供进一 步指南 。

A. 11. 5. 2 “一般要求”指南

附录 C 给出了从非可编程技术迁移到 PE技术时的考虑 。

A. 11. 5. 2. 1 选择SIS中使用的设备和子系统时有一些考虑。首选是按GB/T 20438. 2— 2017和GB/T 20438. 3— 2017设计的部件。第二选择是在有效寿命中使用在类似服务和类似环境中经广泛使用已知是可靠的器件和子系统。有效寿命是指某设备的失效率保持基本恒定的一段时间。SIS中总PFDavg(宜满足通过SIS实现每个SIF的SIL要求)的概率计算以这些失效率为基础。有效寿命结束后,失效率可能会逐渐上升例如由于老化。

无论选择哪个选项,都宜论证设备或子系统:

a) 充分可靠足以达到总的目标PFDavg或者仪表安全功能的目标危险失效率;

b) 满足结构化约束要求;

c) 系统故障的可能性足够低;

d) 在使用电气设备的情况下,它们具有适当的失效率或以往使用为基础。

只要符合GB/T 20438. 2— 2017和GB/T 20438. 3— 2017或者GB/T 21109. 1— 2022的11. 5. 3中以往使用的要求就能满足c)的要求。

一种选择用于安全应用的各种设备的实用方法是,将符合性证据与GB/T 20438. 2— 2017、GB/T 20438. 3— 2017以及操作经验结合使用。这一方法确保所选择的设备是为安全应用设计、制造和管理的,并能够在预期应用中成功运行(例如,应用程序导致的故障被考虑在内)。

证明某设备符合GB/T 20438. 2— 2017和GB/T 20438. 3— 2017的程序不包括过程接口、装置、电源潜在危险失效模式的考虑,或者通信接口可能不包括全部的设备范围,并且有时会受到该设备E/E/PE部分的限制。与过程接口有关的失效对传感器起着非常重要的作用,包括引压管路的堵塞、冻结、腐蚀和气体聚集,在阀门中,则包括阀座损坏、堵塞、沉积和腐蚀(包括阀杆结垢)。正因为这一点,宜对按GB/T 20438. 2— 2017和GB/T 20438. 3— 2017开发的设备进行评价,以确保该设备在其预期应用中运行。这可能包括收集以往使用信息或统计样品的模拟测试。

在选择设备时,用户还宜考虑如何预防系统失效。对于根据GB/T 20438. 2— 2017和GB/T 20438. 3— 2017开发的某设备,有很多宜在设备开发过程中由制造商实现的技术和措施来降低发生系统失效的可能性。另一方面,基于大量文件记载经验并在给定应用中具有给定产品的以往使用历史可用于证明预期应用方面的危险系统失效足够低,因此能充分地预防它们。

A. 11. 5. 2. 2 未提供进一步指南。

A. 11. 5. 3 “根据‘以往使用’选择设备的要求”指南

A. 11. 5. 3. 1 许多用户都有一份被认可和被推荐可在它们的设施中使用的仪表的清单。那些执行情况不理想的传感器和阀门被剔除在清单之外。

这些设备的评估宜包括设备版本的考虑,这些考虑宜得到现场性能监测文档的支持。此外,制造商宜有一个修改过程,以评价已报告的失效和修改的影响。

ISA TR 84. 00. 04: 2015和NAMUR推荐NE 130(“用于SIS的‘以往使用’设备”)给出了以下指南,即如何证明现场设备合格、如何保持它们处于变更管理控制状态、如何观察和用文件记录它们的性能。结果可以在某设备审批表格中收集。

如果没有这样一份列表,用户和设计人员就需对传感器和阀门进行一次评估,以确保它们满足要求,并确保该设备按要求执行。可能需要同其他用户或设计人员进行讨论,以便了解在类似应用中它们正在使用何种产品。

A. 11. 5. 3. 2 宜注意到对一些比较复杂的设备而言,要表明在某个应用中取得的经验是相关的将变得比较困难。例如,就PLC而言,在使用简单梯形逻辑的某个应用中获得的经验,与使用复杂计算和顺序的应用可能并不相关。

一般,现场设备操作上的相关方面与逻辑解算器的不同。

对现场设备而言,以下几点决定其操作特性:

- 功能性(如测量参数 、动作)；
- 操作范围；
- 过程属性(如化学属性 、温度 、压力)；
- 过程连接 。

对逻辑解算器而言，以下几点决定其操作特性：

- 硬件版本和结构；
- 嵌入式软件版本和配置；
- AP;
- I/O组态；
- 响应时间；
- 过程要求率 。

对所有设备而言，以下两点决定其操作特性：

- EMC;
- 环境条件 。

A. 11. 5. 3. 3 未提供进一 步指南 。

A. 11. 5. 4 “根据‘以往使用’选择 FPL可编程设备(如现场设备)的要求”指南

A. 11. 5. 4. 1 未提供进一 步指南 。
A. 11. 5. 4. 2 未提供进一 步指南 。
A. 11. 5. 4. 3 未提供进一 步指南 。
A. 11. 5. 4. 4 本条说明确定 FPL可编程设备是否具备 SIL3能力时的附加要求 。

A. 11. 5. 5 “根据‘以往使用’选择 LVL可编程设备(如逻辑解算器)的要求”指南

A. 11. 5. 5. 1 未提供进一 步指南 。
A. 11. 5. 5. 2 未提供进一 步指南 。
A. 11. 5. 5. 3 未提供进一 步指南 。
A. 11. 5. 5. 4 未提供进一 步指南 。
A. 11. 5. 5. 5 未提供进一 步指南 。
A. 11. 5. 5. 6 未提供进一 步指南 。

A. 11. 5. 6 “选择 FVL可编程设备(如逻辑解算器)的要求”指南

未提供进一 步指南 。

A. 11. 6 现场设备

A. 11. 6. 1 未提供进一 步指南 。
A. 11. 6. 2 未提供进一 步指南 。
A. 11. 6. 3 未提供进一 步指南 。

A. 11. 7 接口

A. 11. 7. 1 “概述”指南

到一个 SIS的用户接口是操作员接口和维护/工程接 口 。SIS和操作员显示器之间交流的信息或数据既可能同 SIS有关 ,也可能是资料性的 。

如果操作员的某个动作是 SIF的组成部分，则宜把执行该动作所需的任何事情都看作是 SIF的 一部分 。例如一个报警指示操作员必须停止过程，在此例中，停车开关(实现停车动作的方式)宜被认为是SIF的一部分 。

不是 SIF组成部分的数据通信(例如，在 SIF 内的跳闸功能执行后，SIF传感器实际值的显示)，如果表明 SIF不会受到影响，则可在 BPCS中显示(例如在 BPCS上只读访问)。

A. 11. 7. 2 “操作员接口要求”指南

在操作员和 SIS之间用于通信信息的操作员接口可包括：

— 显示画面；

—包含指示灯 、按钮和开关的面板；

—声光报警器(可视和可听)；

— 打印机(不一定是通信的唯一方法)；

— 上述的任何组合 。

a) 视频显示器

如果 BPCS视频显示器显示的只是信息数据，则它可共享 SIS和 BPCS的功能 。 通过 SIS可附加显示安全准则信息(例如，如果操作员也是安全功能的组成部分)。

当在紧急工况中需要操作员动作时，宜按照安全要求规范来实现操作员显示器的更新和刷新率。

与 SIS有关的视频显示需能清晰地识别，使之在紧急情况下能避免可能引起操作员误判的不明确性或潜在可能性 。

BPCS操作员接口可用来提供 SIF和 BPCS报警功能的自动事件记录 。

宜记录的工况可包含：

— SIS事件(比如跳闸和并发预跳闸)；

— 每当改变程序而访问 SIS时；

—诊断(如差异等)。

值得注意的是借助报警和/或操作规程可警示操作员 SIS任何部分处于旁路状态 。例如，旁路阀上的限位开关检测到 SIS最终元件旁路，则触发控制面板上的 一 个报警 。 或者通过操作规程管理在旁路阀上安装密封件或机械锁，也可检测 SIS中最终元件(例如截止阀) 的旁路 。通常建议这些旁路报警器保持同 BPCS分离 。

b) 面板

面板宜安放在操作员容易达到的地方 。考虑面板的位置时，宜考虑到某些区域是否会受到潜在危险的影响 。

面板上的布置宜保证按钮 、灯 、规格和其他信息的布置不会使操作员发生混淆 。各个过程单元或设备的停车开关外观类似并分在一组，会导致在紧急情况下处于紧张状态的操作员可能停错设备 。 因此各停车开关宜在形体上加以区分，并标记好各自的功能 。宜提供测试所有灯的方法 。

c) 打印机和 日志记录

与 SIS连接的打印机在出现故障 、掉电 、断开连接 、缺纸或异常行为时，不危及 SIF。

利用时间和日期标记以及位号标识，打印机可用来记录事件发生的时序 、诊断 、其他事件和报警 。宜提供报告的格式化工具 。

如果打印是一个缓存功能(信息被存储，然后在要求时或根据一份定时打印的时间表打印)，则宜规定缓存的容量使之不会丢失信息，以及不存在因缓存空间被占满而危及SIS功能性的情况。

宜在一个显示画面上向操作员提供足够的信息，以便迅速传送关键信息 。显示的一致性是重要的，所使用的方法 、报警约定和显示器件宜同 BPCS显示画面一致 。

还宜注意显示画面的布置 。宜避免在一个显示画面上安排大量信息，因为它们可能导致操作员读错数据和采取错误的动作 。彩色闪光指示灯和适宜的数据间距宜被用于指引操作员到重要信息上 ,从而减少混淆的可能性 。信息宜清楚 、简明扼要和无歧义 。

显示画面设计宜使得有可能是色盲的操作员也能辨认出数据 。例如 ,也可用充满或者未充满的图形来显示由红色或绿色所代表的工况 。

A. 11. 7. 2. 1 未提供进一 步指南 。
A. 11. 7. 2. 2 未提供进一 步指南 。
A. 11. 7. 2. 3 未提供进一 步指南 。
A. 11. 7. 2. 4 未提供进一 步指南 。
A. 11. 7. 2. 5 未提供进一 步指南 。
A. 11. 7. 2. 6 未提供进一 步指南 。
A. 11. 7. 2. 7 未提供进一 步指南 。

A. 11. 7. 3 “维护/工程接口要求”指南

A. 11. 7. 3. 1 未提供进一 步指南 。
A. 11. 7. 3. 2 未提供进一 步指南 。
A. 11. 7. 3. 3 维护/工程接口包括 SIS编程 、测试和维护工具 。接口是用于下列功能的设备：

a) 系统硬件配置;
b) 应用程序开发 、文档编制和下载到 SIS逻辑解算器;
c) 为了更改 、测试和监视而对 AP进行的访问;
d) 查看 SIS系统资源和诊断信息;
e) 更改 SIS安保等级以及访问 AP变量 。

维护/工程接口宜能显示所有 SIS设备(例如作为输入模块 、处理器) 的操作和诊断状态 ,包括它们之间的通信 。

维护/工程宜提供将 AP复制到备用存储媒体上去的一些手段 。

与 SIS连接的 、用于维护/工程 目 的的个人计算机 ,在出现故障 、掉电或断开连接时不宜危及安全功能 。

A. 11. 7. 3. 4 未提供进一 步指南 。

A. 11. 7. 4 “通信接口要求”指南

A. 11. 7. 4. 1 只要维护/工程接口不能用于操纵过程 ,那么两个接口看起来相同是可以接受的 。维护/工程软件不宜作为操作员接口使用 。

A. 11. 7. 4. 2 未提供进一 步指南 。
A. 11. 7. 4. 3 未提供进一 步指南 。
A. 11. 7. 4. 4 未提供进一 步指南 。

A. 11. 8 “维护或测试设计要求”指南

A. 11. 8. 1 设计 SIS宜考虑怎样维护和测试系统 。如果要在过程运行的同时测试 SIS,设计不宜要求断开线路 、使用跳线或者强制软件寄存器(例如 ,输入 、输出) ，因为使用这些技术可能要危及 SIS的完整性 。为了安全地完成包括传感器 、逻辑解算器和最终元件在内的整个系统的测试，系统设计宜提供 SIS的技术要求和规程要求 。

定义怎样在过程运行的同时维护一个 SIS是重要的 。例如 ,如果一个变送器或阀门需要持续运转 ,则宜提供有关在保持过程安全的同时维护部门怎样处理这些仪表而又不会引起跳闸的考虑 。

对最终元件测试周期的任何限制都宜在计算 SIF的 PFDavg时加以考虑 。

A. 11. 8. 2 未提供进一 步指南 。

A. 11. 8. 3 安装旁路可能降低一个 SIS的安全水平 。通过以下办法可以克服这种安全性的降低 。

a) 使用口令和/或键锁开关 。有些设计可结合带锁机柜内装适当的旁路 。

b) 通过对阀门位置加封或者设置指示相应位置的重要性的安全符号 ,清楚地标识管道旁路 。

c) 用于控制旁路应用和移除的清除程序或设施(例如 ,控制旁路移除开关) 。

d) 使用具有能自动移除旁路时间限制功能的旁路 ,此特征降低了旁路在完成测试或维护后仍保持活动的风险 。

例如 ,对一个 1oo2传感器配置而言 ,有些用户可能同时旁路两个传感器 ,而另一些用户可能对每个传感器单独旁路 。如果同时旁路传感器 ,则必须使措施到位以保证风险保持在可允许的范围 。两种情况都有可能 ,宜在设计初期就对此进行讨论 。

同样 ,有一些过程操作不支持在过程运行期间移动阀门 ,或可能在阀门周围安装旁路不现实 。在这些情况下 ,设计宜尽量使 SIS实际可测试 ,也就是说 ,至少通过电磁阀 。在这种情况下 ,设计中可以包含电磁阀周围的某种旁路形式 ,利用这种旁路常用的报警或者规程控制 。

A. 11. 8. 4 SIS内可设置用于限制旁路持续时间的计时器 ,例如 ,通过自动复位和/或向操作员报警 ; 可在 SIS内提供自动复位任何抑制或超驰控制的逻辑 ,例如泵启动过程中压力不足 。

A. 11. 8. 5 未提供进一 步指南 。

A. 11. 8. 6 强制 PESIS内的输入和输出不得用作 AP的一部分 。例如 ,在运行程序时 ,通过使用程序员工具在线编辑逻辑解算器内的存储器而对输入和输出进行不受控强制经常用于程序开发过程中 , 以便探索 AP的提议修改 。然而 ,这种做法不得在线使用 , 因为它会掩盖工厂变量的 “真实” 输入状态和/或向工厂设备馈送假输出 。在任何一种情况下 ,逻辑解算器不会以预定模式控制该工厂 。此外 ,对应用程序所做的此类小幅修改很容易被忽视 , 当不再要求的时候 ,会仍然保留在程序中 。

A. 11. 9 “随机失效的量化” 指南

A. 11. 9. 1 可用于保证设计满足与硬件随机失效有关的性能的技术指南,用户和设计人员宜参见 IEC 61511-3:2016 的附录 J; GB/T 20438. 6— 2017 的附录 B; ISO 12489; ISA TR 84. 00. 02: 2002; GB/T 20438. 3— 2017的附录 B; IEC 61025(故障树) ; IEC 61078(可靠性框图) ; IEC 61165(马尔克夫图) ;IEC 62551(Petri网) ;IEC 62502(事件树)等 。

在检验测试间隔期间 ,PFD(t)会随着时间的流逝而持续上升 。 因此 ,在它与其平均值相交后 ,它将在平均值上方保持一致 ,直至检验测试间隔结束 。 在某些情况下 , 它还可能会与对应于这 一 平均值的 SIL边界相交 ,并在该值上方保持一致 。 因此 ,在需要较高的安全完整性时 ,这些平均值可能会单独给出假的安全感 ,宜进行验证 ,例如 ,验证对应于峰值的风险是与用户组织机构中的风险准则一致的 。

根据操作要求模式(例如 ,关闭阀门 , 防止过压)动作的 SIF之后通常紧随着相同元件但在连续操作模式中动作的另一个 SIF(例如 ,只要阀门上游出现过压 ,就会防止阀门打开) 。 因此 ,对于根据运行的要求模式动作的 SIF来说 ,宜考虑与 SIS失效相关但不会使过程停留在安全状态的危险频率 。

A. 11. 9. 2 预估失效率可利用来自已识别工业源和之前用于与预期应用相同环境的经验的失效率 ,通过设计的量化失效模式分析确定 。为了保守起见 ,可在计算中使用输入数据 70%的置信上限 。

需要注意 ,故障容错单元的总体未检出失效率与时间有关 ,并在检验测试间隔内随时间逐渐增加 。故障容错单元可能会有时间相关的失效率 。

示例 : 由两个类似元件 A 和 B(未检出失效率 λ相同)构成的某一单元 , 当时间增加时 ,总体未检出失效率 A从 0 上升到λ。

在量化某一 SIS(或其 SIS子系统) 中随机硬件失效的影响时 ,将使得 SIF操作在高要求模式或连续模式中实现的硬件故障裕度为 0 时 ,如果出现以下情况 ,则只能取用于诊断的信任值 :

—诊断测试间隔和执行规定动作以便达到或维持在安装状态的时间之和小于过程安全时间 ;或

— 在高要求模式中 ,诊断测试频率与要求频率之比大于等于 100。

例如 ,检验测试规程和检验测试设施的可靠性分析包括 :

— 检验测试的持续时间 ;

— 检验测试期间的过程(正在运行或已停止的过程)状态 ;

— 检验测试(在线或离线)过程中被测设备的状态 ;如果被测设备在检验测试期间为离线状态(即不可用) ,则这是 PFD_{avg} 的重要影响因素 ;

— 当检验测试不是 100%有效时的检验测试覆盖率 。这意味着需要对本质上永远不能通过检验测试检测的失效进行标识 ;

— 可能由检验测试自身导致的失效(例如由于改变测试用途所需的状态而导致失效) ;

— 为了解除检验测试的关联而可能导致类似冗余设备检验测试错开的现象 ;

— 检验测试返回到 SIS健康状况不正确结果的可能性 :

- 受到检验测试自身相关故障影响的检验测试 ;
- 检验测试过程中的人为错误(例如 ,未检测到实际失效 、遗漏某 一 测试 、检验测试或维修的设备在检验测试或维修完成后仍然维持离线状态等) 。

如果检验测试间隔没有为概率计算明确建模 ,则各检出危险失效的 MTTR 可按照检验测试间隔的一半加上所考虑失效的 MRT。

A. 11. 9. 1 中的大多数技术要求用量化表示 SIS的诊断覆盖率 。诊断测试被自动执行以便检测 SIS中有可能导致安全失效或者危险失效的故障 。

通常一种特殊的诊断技术并不能检测所有可能的故障 。对于所讨论的 一 组故障 ,可提供所用诊断有效性 的 一 个 估 计 (有 关 怎 样 计 算 诊 断 覆 盖 率 的 例 子 见 GB/T 20438. 2— 2017 的 附 录 C 和 GB/T 20438. 6— 2017的附录 C) 。

提高 SIS的诊断覆盖率有助于满足 SIL要求 。在这种情况下 , 当计算 SIS的失效概率(要求模式)或者失效频率(连续模式)时 ,宜考虑诊断覆盖率和诊断测试之间的周期(诊断测试间隔) 。 附加指南可参见 GB/T 20438. 2— 2017的附录 C或者 ISA TR 84. 00. 02。

在 SIS是仅有的保护层并用于连续操作模式下执行某个安全功能的情况下 ,所需诊断测试间隔应使之能及时检测到 SIS中的失效 ,从而保证 SIS的完整性 ,并使之能在过程中或在基本控制系统中发生一次失效事件时采取动作 ,从而保证某个安全状态 。

要实现这一点 ,诊断测试间隔和达到某个安全状态的反应时间之和需小于“过程安全时间” 。根据 GB/T 21109. 1— 2022的 3. 2. 52. 1 过程安全时间被定义为不执行仪表安全功能时 ,从过程中或 BPCS中发生一次失效(具有引起一次危险事件的潜在可能)到发生危险事件之间的时段 。

公共设备的致命的和潜在的致命故障(如 CPU/RAM/ROM故障)典型地几乎完全禁止数据处理 ,因此要远远大于仅一个输出点的故障的影响 。具有高失效概率的失效模式的检测一定要有较高的置信度 。此外 ,宜考虑失效模式的可检测性 。

就被实现的每个诊断程序而言 ,检测故障的测试间隔和导致的动作需满足安全要求规范 。

当这些诊断程序并不是“内装”在供应商提供的设备中时 ,为了满足 SIF的 SIL,可在系统或应用层实现外部配置的诊断程序 。

诊断不能检测系统误差(比如软件缺陷) 。然而 ,采取适当的预防措施 ,也许能实现检测可能的系统故障 。

使用各种方法或者这些方法的组合可实现诊断 ,包括 :

a) 传感器

1) 提供可检测上限或下限已全部失效的一个传感器的诊断报警设备 。其实现方法是使用 一个超量程报警器 。例如 ,在一个使用冗余温度传感器的高温跳闸应用中 ,可附加一个超下限报警器来诊断传感器失效或者传感器信号丢失 。

2) 如果使用冗余传感器 , 通过比较模拟量值可检测正常运行过程中可能发生的异常情况 。

如果使用了 3个传感器，可使用 3个读数的中间值(中值选择，见下面的注)。 因为不能正确执行功能的设备会使平均值跑偏，与平均值相比，中值选择更有优势。下列原因可使读数之间产生重大的偏离：

- 引压管路的堵塞或冻结；
- 冲洗源压力的降低；
- 温度计套管的表面结垢；
- 接地或电源问题；
- 传感器不响应，其输出值始终不变。

注 1: 中值选择比平均值更具优势，因为平均值会偏离不正确起作用的设备。尽管如此，如果两台变送器都给出假的读数，则中值选择会失灵，从而可以考虑共模失效。

3) 如果“2”适用，或者在 SIS 中的模拟传感器与可比过程参数读数之间通过系统中的其他传感器如 BPCS进行比较，则诊断覆盖率的潜在提高由特定应用决定，并且需要进行分析、评价和文件记录。如果声明某一诊断覆盖率高于 90%，则宜分析并记录协同传感器之间的共因失效(CCF)。

注 2: 为了便于进行比较，任何矛盾都至少可以产生一次报警。这一差异报警阈值可根据相关过程变量的文档化偏离来设定。这些比较检测了 SIS传感器和非 SIS传感器二者的失效。然后，在实现这一解决方案之前，可分析由非 SIS传感器失效产生的误警报或误跳闸。

注 3: 提高这一比较类型所提供的诊断覆盖率，可用于延长检验测试间隔。

4) 为防止由于传感器位置或传感器技术引起过程变化，而导致传感器响应变化所产生的误报警，可提供时间延迟。例如，有的冗余流量传感器有 1s~ 2s 的延迟。 为了监视冗余传感器读数和计算标准偏差以使启动诊断报警，厂家可提供许多软件包。

5) 传感器诊断的另一方法是对相关变量(例如，流量累加器与槽液位变化或者压力关系及温度关系)进行比较。

b) 最终元件

1) 可以对最终元件(如限位开关或位置发送器) 的反馈同要求的状态进行比较，从而验证已经采取过预定动作。宜使用足够的延迟以便筛选处于转换之中的阀门(如从全开到全闭)的报警。 只有在阀门定期改变到作为正常工作组成部分的安全状态时(例如分批操作)，才能考虑对最终元件的反馈同要求的状态进行比较。

2) 有些阀门、执行机构、电磁阀和/或定位器也能提供诊断能力。

c) 逻辑解算器

安全配置的或者符合 IEC 61508 的 PE逻辑解算器典型地包含检测各种故障的诊断程序。一般在安全手册中描述有诊断程序的类型和诊断覆盖率。

d) 外部配置的诊断程序

例子包括监视定时器程序和线端监视器。

用于执行目标测量计算的可靠性数据中的置信度，还可根据考虑取值。使用输入可靠性参数 70%的置信度上限值确保执行保守计算，GB/T 21109. 1— 2022 的 11. 9. 4对此进行了讨论。

A. 11. 9. 3 未提供进一步指南。

A. 11. 9. 4 量化随机硬件失效影响时的可靠性数据值通常只能使用数值不确定度才知晓。 因此评估这些不确定度对目标测量值的影响对于合并 SIL声明是非常有用的。

某一给定可靠性参数(例如失效率)的不确定度(见注 1)可通过以下方法评价：

a) 统计分析；

b) 执行专家判定(需要时)；

c) 进行特定测试。

一般来说，当可用现场反馈的数量增加时，数值不确定度会下降。

因此，可靠性参数并不是完全已知的确定值，而是一个随机变量，其分布或多或少分散在其平均值周围，如图 A. 5 中的说明。

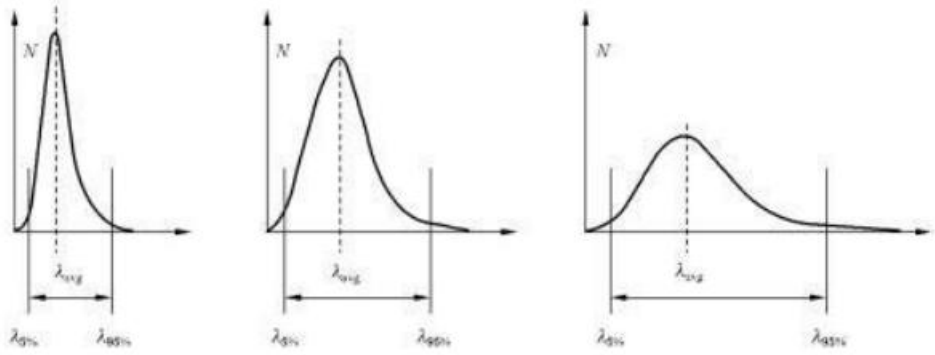


图 A. 5 可靠性参数的不确定度说明

分布越尖锐,参数的不确定性就越小。不确定度在图 A. 5 中从左到右递增。

在极限情况下,如果参数完全已知,则该曲线将为简单的垂直直线(即狄拉克分布)。

如图 A. 5 中的说明,可靠性参数λ 的不确定度可通过其置信水平进行评价,例如,90% :λ 的实际平均值有 90%的可能性属于区间[$\lambda_{5\%}$,$\lambda_{95\%}$],其中λ有 5%的可能性比$\lambda_{5\%}$好,有 5%的可能性比$\lambda_{95\%}$差。

在纯粹的统计基础上,可靠性参数的平均值可使用“最大似然估计”来估计,置信界限[$\lambda_{5\%}$,$\lambda_{95\%}$]可使用在统计书中制成表格的χ^2(卡方)函数来计算。

在累计观察时间 T 内观察到出现 n 次失效的某一样本其平均值等于n/T,90%的置信区间等于$\left[\frac{1}{2T}\chi^2_{0.95,2n},\frac{1}{2T}\chi^2_{0.05,2(n+1)}\right]$当累计观察时间和/或观察到的失效次数增加时(图 A. 5 中,从右向左增加),此区间的宽度会缩小。

还可使用贝叶斯方法处理统计观察值、专家判定和特定测试结果。可以使用这一方法拟合相关的概率分布函数,以便进一步用于蒙特卡罗模拟。

当置信区间较宽时(即在现场反馈比较稀疏的情况下),宜尽快实现可靠性数据收集过程,并且利用已收集的可靠性数据定期更新目标概率测量值的概率预测。

注 1: GB/T 21109涉及到需要执行准确可靠性数据的概率计算。如果未从用户处收集可靠性数据,则不能正确实现这一计算。在确定缺乏可靠性数据时,为了填补这一空白而启动特定的可靠性数据收集是一次机会。如果不能用于现在的 SIS,则可用于下一个。

处理上述不确定度的第一种方法是使用悲观输入可靠性数据。这保证即使在缺乏准确度的情况下,目标测量值(PFD_{avg}或 PFH)的评价是不乐观的。这可以通过用于输入可靠性参数的置信上限值(高于传统的平均值)来完成。通常会考虑使用 70%的上限(例如,$\lambda_{70\%}>\lambda_{avg}$)来给出合理的置信水平。这在图 A. 6 中进行了说明,图中表明,当准确度提高时输入数据的保守程度降低($\lambda_{70\%}-\lambda_{avg}$之差降低)。

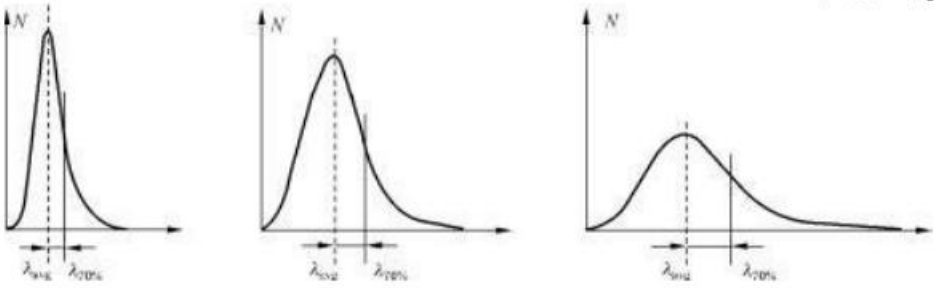


图 A. 6 70%置信度上限的图解

注 2: 在累计观察时间 T 内，出现 n 次失效的某一 观察样本中，置信上限可用χ^2 函数计算：例如，$\lambda_{70\%}$ 可通过$\lambda_{0,7} = \frac{1}{2T}\chi^2_{0,3,2(n+1)}$ 评价，有 70%的机会是实际值低于(或优于)该值 。 即使在没有观察到任何失效时，这 一 置信上限仍然存在 。与 λ_{avg}相比，它通常是保守的，但当 T 和/或 n 升高时，其保守程度会越来越低(见图 A. 6) 。

注 3: 用输入参数 70%的置信上限执行计算不会给出总结果(例如 PFD_{avg})70%的置信上限 。通过这种方式完成的计算仅仅保证该结果是保守的 。

上述方法暗示只对概率目标(即 PFD_{avg}) 进行了 一 次计算，但保守水平未知 。 因此，如果需要知晓这一保守水平,则可能需要使用另一种方法。 这包括使用输入可靠性参数的整体分布而不仅仅是像 $\lambda_{70\%}$ 一样的单个值 。所谓的“蒙特卡罗”模拟可用于：

a) 使用随机数模拟输入可靠性参数值的概率分布;

b) 使用不同随机数集实现概率目标的几次(例如 100次)计算 。

这提供了目标结果(例如，PFD_{avg})的统计样本(即柱状图)，可对该统计样本进行处理，以便获得相应的概率分布以及相应的平均值和置信水平(见图 A. 7) 。

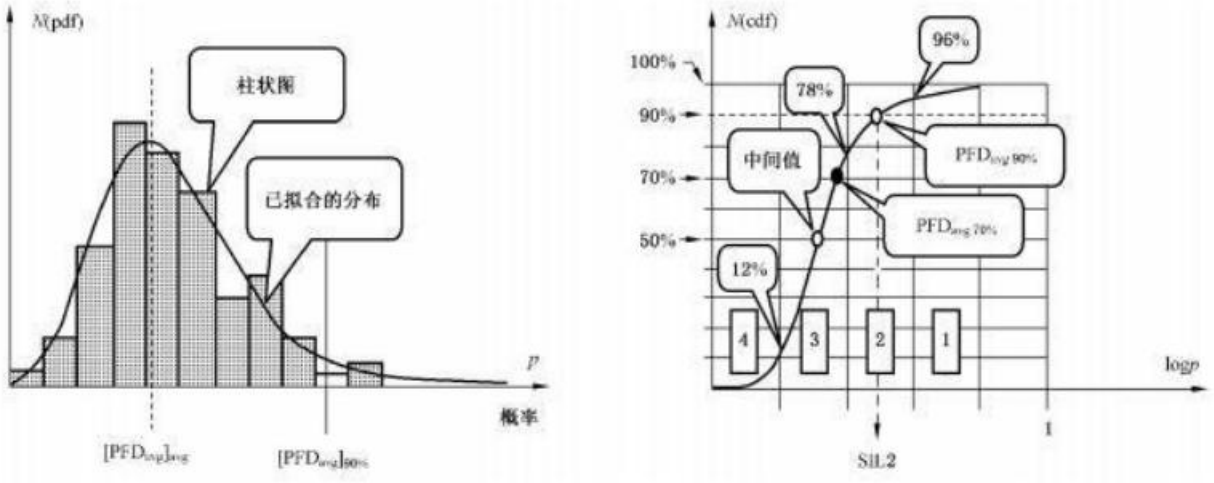


图 A. 7 根据蒙特卡罗模拟得出的目标结果的典型概率分布

图 A. 7对可以根据蒙特卡罗模拟获得的概率密度函数(pdf)和相应的累计分布函数(cdf)进行了说明 。这表明 PFD_{avg}分布在它的平均值[PFD_{avg}] $_{avg}$周围 。

注 4: 由于使用了基于概率法则进行计算，因此 PFD_{avg}本身是一个随机变量 。上述计算仅仅从本质上给出了由于输入可靠性参数的不确定度造成的分布 。

可以使用[PFD_{avg}] $_{avg}$而不是经典的 PFD_{avg}，但不能证明它的保守性 。可能会接近中值(即实际值优于(PFD_{avg})50%的概率是 50%，剩余 50%的概率是实际值会更差) 。

图 A. 7 中 cdf曲线表明，PFD_{avg}处于 SIL4相关范围内的概率为 12%(剩余 88%的概率是处于 SIL3或更糟糕的范围内)，处于 SIL3或更好范围内的概率为 78%(剩余 22%的概率是处于 SIL2或更糟糕的范围内)，处于 SIL2或更好范围内的概率为 96%(剩余 4%的概率是处于 SIL1或更糟糕的范围内)等 。

为了保守起见，可以选择 90%的置信水平 。 因为[PFD_{avg}]90%处于 SIL2的限值内，这会导致其完整性水平为 SIL2。请注意，如果使用 70%的置信水平，则在同一例子中，则会给出 SIL3的完整性水平 。

A. 11. 9. 5 未提供进一 步指南 。

A. 12 SIS应用程序开发

A. 12. 1 目的

关于如何为 SIS中的一个或多个 SIF开发 AP的例子，见 B. 1 和 F. 20。

A.12.2 “一般要求”指南

A.12.2.1 GB/T 21109.1— 2022的第 12章适用于开发和修改各种要求达到 SIL3的 AP。经验表明，当根据相应的安全手册使用有限可变语言(LVL)为符合 GB/T 21109.1— 2022要求的逻辑解算器开发AP时 ,SIL1、SIL2或 SIL3的开发方法几乎没有区别 。

对不同 SIL的测试和验证技术,在 SIL1、SIL2和 SIL3之间可能会有差异 。见 A.7.2.2。

A.12.2.2 例如,应用程序员宜审核逻辑描述(例如,F.15和 F.17)中的信息与作为过程一部分的顺序指令,以检测缺陷并确保应用程序员理解预期的要求 。

A.12.2.3 GB/T 21109仅限于对使用有限可变语言(LVL) 开发 AP 的要求,“AP开发”被解读成为按照 GB/T 21109.1— 2022的 11.5要求选定的 PE来设计和实现应用安全逻辑 。

A.12.2.4 GB/T 21109还提到了使用固定程序语言(FPL)设备的应用,例如对智能传感器中参数的输入进行控制,关于示例,见附录 C 和表 F.13。

A.12.2.5 隔离非安全性应用程序和 SIF应用程序 。

证明可能存在充分独立性的一种方式是遵循下列所有的要求：

a) AP中的 SIF清晰地标识为 SIF应用代码 ；
b) 将 AP中的非 SIF清楚地分开 ；
c) 标识出 SIF实现过程中使用的所有变量 ；
d) 所有实现非安全仪表功能的 AP标识为非安全仪表功能代码 ；
e) 所有 AP用非安全变量和 SIF变量都满足以下条件 ：
f) 非安全 AP(包括所有的功能和功能块)不写入安全 AP所用的任何 SIF变量中;以及
g) SIF实现过程中,安全 AP不依赖于任何非安全变量 ；
h) 保护所有安全 AP(包括变量和数据),避免受非安全 AP变更的影响 ；
i) 如果安全和非安全 AP共享相同的资源(例如,CPU、操作系统资源、存储器、总线),则决不能损害安全 AP的 SIF(例如,响应时间) 。

A.12.2.6 见 A.11.2.8中的指南 。如果 AP不包括手动复位,则宜在 SRS中确定这一点 。

对 SIS失电、供电恢复但不能维持过程安全状态的可能危险进行说明 。另请参阅 GB/T 21109.1— 2022的 A.11.2.8和 12.2.5。在得电跳闸的情况下,请参阅 GB/T 21109.1— 2022的11.6.2。

A.12.2.7 未提供进一 步指南 。

A.12.2.8 确保每次扫描时对所有的输入和输出进行刷新,降低 AP的复杂程度。 另请参阅 ISA TR 84.00.09。它还有助于确保达到响应时间要求,见 GB/T 21109.1— 2022的 10.3.2。

A.12.2.9 确保使用适当的 AP。宜考虑参照操作和监管要求必须安全存储和检索多长时间的旧版本 。还宜考虑运行旧版本的 AP所需的支持硬件和嵌入式软件 。在实现 AP 的任何修改之前,宜验证机器中的 AP运行与原版拷贝完全相同 。在恢复用户数据之前,宜验证用户数据是适当的版本 。见5.2.7。

A.12.2.10 未提供进一 步指南 。

A.12.3 “应用程序设计”指南

A.12.3.1 操作模式可包括许多操作功能,如手动、半自动 、自动、起动、批量、测试和维护功能 。见F.14和 F.27。

A.12.3.2 关于 AP设计输入的例子,见 F.13。关于 SIS用 SRS的例子,见步骤 F.3。F.20和步骤F.3中给出了用于开发 AP设计的方法和工具示例 。

应用程序员与 SIS设计人员可能有必要讨论 AP设计输入 。

A.12.3.3 为了便于进行 FSA,AP宜可追溯至 SIS的安全要求规范 。 例如,通过它表明如何实现 SIF的方式来构筑,标识符宜反映实际的装置— 通过使用“真实世界”的输入/输出标识名 。AP还宜带有

体现过程功能的注解 。也可参见 GB/T 21109. 1— 2022的 5. 2. 6 和图 F. 11中的例子 。AP设计宜描述 AP的设备和 SIS子系统 、它们之间如何互连 、怎样达到所要求的属性特别是安全完整性 。 AP设备的例子包括在整个程序过程中复制的应用功能(例如 ,泵的控制顺序) 、与工厂 I/O 和通信模块的信息交换 、与底层 PE设备互相关联的 AP层功能(例如 ,使用多个 SIS来实现冗余功能和/或错误检测行为以及/或起动/关断顺序) 。

执行 AP的 FSA有助于在较早阶段识别错误 ,并且保证 AP在失效方面具有鲁棒性 。AP 的 FSA 可包括 :

a) 确认 AP符合安全手册的限制 ，以及任何特定的应用程序编码标准和安全编程实践;

b) AP行为的失效分 析;这 包 括 AP所 执 行 功 能 的 识 别 、它 们 潜 在 的 功 能 偏 差(例 如 , 像 在 化 学 HAZOP中一样 ,太大/小 、太早/晚 、对立/不存在/无等) 、每个应用功能的失效影响评估以及针对出现功能失效的任何缓和措施的识别 。

注 :很多 AP功能为 SIF, 因此失效分析可作为系统失 效 分 析 的 一 部 分 进 行;然 而 , 为 了 避 免 SIF失 效 , 可 能 已 经 在 AP中 识 别了附加功能或者可能在功能失效分析本身的过程中识别了附加功能(例如 ,控制泵 、对诸如消防和燃气或温度和压力等过程输入进行表决 、对故障采取行动) 。

A. 12. 3. 4 下文给出了用于应用程序设计的技术示例 。

a) 见图 F. 11的第 4 页 ,第 1行 。

b) 见 F. 20的 AP例子(表 F. 8~表 F. 14);AP结构宜与该过程的结构 一致 。 (例如 ,在化工厂内 , 用于每个过程装置的 AP宜分在 一起 ,在每个过程装置内 ,设备之间是分开的 ，以便于理解和维护) 。

c) 网络和逻辑的正确执行顺序宜在每个程序中定义 ,还宜定义所有 AP 的执行顺序和期望执行速率 。宜确认 AP的执行速率与 AP的 SRS规定的过程响应时间一致 。

d) 在图 F. 11的第 1 页中 ,可以找到标准库模块的描述示例 。

e) 在 B. 4. 1 中 ,可以找到特定库模块的描述示例;宜设计自定义功能块 ,使重复的操作便于编程 、测试和重复使用 ,I/O模块和内存可变数据区需配置 。

f) 在 PLC 中执行应用程序编程时 ，内存分配通常是自动完成的; 内存分配是通过将 AP 的各个部分(例如 ,报警 、输入 、输出 、安全逻辑 、非安全逻辑 、未来增长的空白空间)划分到各自的梯级上来实现的— 见图 F. 11的例子;如果必需手动完成划分 ,则在存储管理的过程中 ,宜注意以下方面 :

- 将等效变量分布在专门的页码中 ，避免将常数与变量 、输入与输出 、物理变量与中间变量混淆;
- 将不同变量类型分开 ,避免将实数 、整数和二进制数混淆;
- 遵循每个变量一个内存地址的规则 ,避免在更复杂的变量类型中复用简单变量类型 ,例如在整数或字节中嵌套多个二进制变量 。

g) 应用程序全局变量的一个例子可以是安全警报 ,例如根据正在处理的批量成分改变高温警报;另一个例子可以是用于消防和瓦斯保护系统的高可燃气体警报限值— 例如 ,20% 爆炸限值下限(LEL);完整性保护的例子可以是底层逻辑解算器的功能 ,它可能限制全局变量只能被 一个 AP 指令覆盖;在 G. 3. 4. 3、G. 3. 4. 4、G. 7. 2. 4、G. 7. 3. 1 和 G. 7. 3. 2 中 ,可以找到使用全局变量的其他考虑 。

h) 将安全和非安全功能分成多个单独程序是可取的 ,这样可以将重点放在安全程序上 ,并且可以很容易地证实非安全功能不会干扰安全功能; 图 B. 13给出了 SIF与 非 SIF独 立 性 分 析 的 例子;SRS宜规定某一 给定程序中包括哪些 SIF和其他功能;宜将安全方案的规模限制在少数功能上 ，以便最高程度的完整性只适用于基本的安全功能 。

i) 图 F. 11第 1 页和第 2 页给出了输入和输出描述的示例;宜开发所有 I/O 和存储器变量的标

识名 。

j) 图 B. 6 和 B. 12给出了 SISHMI规范的例子 。

k) 宜确定 SIS外围系统的通信变量;如果这些变量为内存变量 ,则需要将它们分配到合适的数据区域 ,这样就可以通过 SIS通信子系统访问;宜仔细定义可通过 SIS外部的其他系统修改的变量 ,这些变量通常宜放在存储器专门的读/写区域中;图 B. 13说明了 SIS与 BPCS之间的数据交换示例 。

l) 需要确定传感器与最终元件的诊断程序和定期测试原理;这些诊断程序和定期测试原理与传感器和最终元件冗余有关;测试原理需要仔细定义 ,并宜包括测试时间段内适当的报警程序 ;图 F. 11第 3 页的第 A1行至第 A6行 、第 4 页的第 4、6、8、10行以及第 5 页的第 17至 20行是诊断程序的示例 。

m) 需要仔细说明警报的处理和记录及其对风险降低的影响;还需要进 一 步确定维护超驰控制的方法;一些用户会要求通过数字输入点对开关进行线连接 ，以便启动维护超驰控制 ，而其他用户会使用来自显示站输入 SIS的受控数据;无论在哪种情况下 ,都要求执行安保程序 ,避免出现意外超驰控制/旁路;关于报警图的典型例子 ,见图 F. 11第 3 页;关于报警的优先次序 ,见附录 F. 14和表 F. 13;关于操作员界面的典型例子 ,见图 F. 11第 2 页的第 DI1、DI2和 DI3行 。

n) 应用数据完整性检查和传感器确认的例子包括 ：

- I/O数据的超量程检查 ,例如 ,超量程变送器 ；
- 应用通信数据的确认 ,例如 ,外部看门狗定时器 、外部循环冗余检查(CRC)算法 ；
- 传感器值的比较和偏差报警 。

o) 系统配置检查可以通过结构测试进行(详细的结构测试说明见 12. 5. 3 b) ,此外还需要注意确保位号名称等是唯一 的 ,包括在控制器之间 。

p) B. 3. 2. 2. 1 中给出了复杂性控制的一个例子 ,其中某 一 AP的复杂程度受到使用三层模块中分层组织结构的限制(另请参阅图 B. 9) 。

q) 图 F. 11第 3 页的 D01、D02和 D03行 ,第 4 页的第 1行和第 2行 ,第 5 页的第 12行和第 16行至第 20行显示了 SIS和 SIS子系统 I/O故障的管理示例 。

r) 物理输出的部分行程测试是用自动抑制进行在线测试的一个例子,另见A. 16. 3. 1. 2和A. 16. 3. 1. 3。

s) 图 B. 6 给出了用于离线测试的维护开关接口示例 。

t) 对 SIS的修改需离线完成— 修改过程的安全通常依赖于以下因素 。

- 防止对逻辑解算器内的 AP进行在线修改;这通常通过借助硬件开关和密码来达到 ；
- 防止访问 AP下载链接 ；
- AP工作平台的固有特性及其嵌入式安全特征 ,包括语法控制 、一 致性检查 、可追溯性和版本控制 。

u) AP安全要求规范通常包含在某一文件或一组文件中 ,这些文件经过分层组织 ，以便逐步细化多个要求(从 SRS到最详细的实现规范 ,如内存映射) 。对于 SIS来说 ，由逻辑解算器提供的 AP文献资料不是充分的 SRS。

A. 12. 3. 5 正确应用编程设计的考虑包括 ：

a) 见 F. 17和 F. 27。

b) 所实现的 AP宜实现 AP安全要求规范中所述的所有功能 ,宜确定其他所有未规定的行为 ,且不得损害安全完整性 。

c) 关于避免模糊不清的指南 ,见 A. 12. 6 和附录 G。AP宜以帮助操作员和维护人员理解 SIS并与 SIS交互(要求时)的方式实现 。例如 ,报警显示 、所要求的响应时间 、操作员的工作量等的描述 。各功能宜支持维护活动 ,包括使用超驰控制和旁路 。

d) 关于达到无设计故障的指南,见 A. 12. 6。

A. 12. 4 “应用程序的实现”指南

A. 12. 4. 1 只要有可能,AP宜以经过充分证明的 AP模块为基础,这些模块可包括用户库功能和用于连接 AP模块并经过良好定义的规则(见 B. 4. 3. 3. 1、B. 4. 3. 3. 2. 1、B. 4. 3. 4. 1 以及图 B. 9)。 在图F. 11第 1 页中,给出了一部分 AP(使用了供应商提供并经过安全评估的库功能块)的例子 。

A. 12. 4. 2 如何实现第 1部分的各项要求,请参阅以下参考信息 。

注 :附录 F是基于 IEC 61508和 IEC 61511的 2016版的一个例子 。

a) AP创建人,图 F. 11的底部,标题框;

b) AP 的用途描述:F. 1、F. 2、F. 3、F. 4 以及 F. 5. 1 和 F. 5. 2;

c) 未提供进一 步指南;

d) 未提供进一 步指南;

e) 向 AP SRS的追溯,表 F. 12;

f) 每个 SIF及其 SIL的确定,表 F. 11;

g) 所使用符号的识别和描述,包括逻辑约定 、标准库功能 、应用库功能,图 F. 11第 1 页;

h) 关于 SIS逻辑解算器输入和输出信号的识别,见表 F. 9 和 F. 10;

i) 在整体 SIS利用各种通信的情况下,关于通信信息流的描述,见图 F. 12;

j) 关于程序结构的描述,包括数据在输入/输出 SIS子系统方面的逻辑处理顺序描述,以及关于由扫描次数产生的典型限制条件,见 B. 1;

k) 确保现场数据和数据正确发送至通信链路的方法(如果 SIF规范要求) — 见图 F. 11第 5 页的第17、18、19、20行;

l) 关于版本识别和变更历史,见图 F. 4、F. 5、F. 6、F. 7、F. 8、F. 9、F. 10、F. 11中每一页的底部。

A. 12. 4. 3 AP库功能的重新使用宜证实能在类似的应用中进行令人满意的操作,包括相同的库功能已经证实能在类似使用条件下进行令人满意的操作的证据 。先前开发的应用于许多过程设施的应用程序库函数的一个例子是一个应用程序模块,该模块执行了瞬间三线制电机控制功能中的启动 、停止和密封功能。

A. 12. 4. 4 为了构建一个健壮可靠的 AP,宜考虑其结构 。这可能包括在底层逻辑解算器设计中增加应用层面冗余的方式,在多个 I/O之间共享功能(如阀门控制结构),以及输入和输出变量处理顺序 。

A. 12. 5 “应用程序验证(审查和测试)要求”指南

A. 12. 5. 1 未提供进一 步指南。

A. 12. 5. 2 此处的能力是指人员具有专业技术背景和教育(例如,学士或硕士学位或同等学历),熟悉所使用的程序语言和设计及实现工具,是经验丰富的应用程序程序员 。此外,他/她宜具备功能安全知识,特别是对过程工业领域 。他/她宜能够识别本质上不安全的逻辑(例如,失电安全状态应用中的“或”门或反相,或者通电安全状态应用中的与门)。见 F. 28。

A. 12. 5. 3 在测试过程中,宜覆盖 AP中所有的区域,以保证正确运行,并确保应用中的某一 区域不会对程序的另一部分产生不良干扰 。宜在完全允许的整个范围内对数据进行检查,从而确保系统在量程内将正确地运行 。还宜进行超出范围的检查,以确保检测到超出范围的数据并采取适当的行动 。并且宜进行测试,以确认 AP未执行危害其安全要求的非预期功能 。

AP审核宜包括诸如审查 、走查和形式化分析等技术 。 审核宜结合仿真和测试 一 起使用,以保证 AP符合其相关的规范 。

测试可以为“黑盒”测试(在不知道 AP 内部结构的情况下进行的测试),例如,功能测试或“白盒”测试(知道 AP 内部结构的测试)。在这两种情况下,证实测试结果符合需求是非常重要的,但在白盒测试

的情况下,则可更容易地识别“意外”行为 。

AP测试最初可在某一模拟器上进行 ,然后可在逻辑解算器硬件上根据设计和要求规范阶段内产生的规范进行 。最初测试阶段(根据设计规范进行模拟和测试)的目的是 :

a) 证实 AP模块提供了必需的功能 ,且不会执行任何禁止的行为 ;

b) 使 AP经受大范围条件和顺序的影响 ,从而表明它能从非预期行为中复原 ;

c) 结构测试包括 AP开发和测试的三个关键阶段(单元 、集成和系统测试) 。

AP结 构测试是为了在结构和设计逻辑的基础上用测试用例挑战 AP所做的决定 。完整的结构化测试在下面讨论的测试级别上演练 AP 的数据结构(如配置表 、典型值 、子例程 、函数) 及其控制和过程逻辑 。

结构测试宜在单元测试 、集成测试和系统级测试中进行 。此处使用的 , “单元”是代码的最小单独可编辑或等效的设计 ,例如过程 、子例程 、类 、方法或数据库表 。结构化测试确保 AP的语句和决策通过代码充分执行 。例如 ,它确认 AP循环构造在其数据边界上的行为符合预期 。对于可配置 AP,将评估配置表中数据的完整性对程序行为的影响 。在单元级别 ,结构测试还包括 “死代码”的识别 ,这是任何代码路径都无法到达执行的代码 。

完成所涉及单元的全部验证测试之后 ,在系统等级的结构测试之前 ,宜执行集成结构测试 。AP验证确认 AP开发每个阶段的输出都忠实于(即符合)该阶段的输入 。性能测试确认在预期硬件和环境中运行的最终 AP与设备技术规范和 AP要求规范中规定的预期用途一致 。

—单元等级的结构测试

单元根据需要会被编译并与驱动程序和存根程序连接 。驱动程序是最终调用被测单元的任何实际单元的代用品 ,如果该驱动程序将数据传递到被测单元中 ,则它将被设为传递测试用例变量值 ,如最大值 、最小值以及其他标称值和压力测试值 。存根代码是被测单元调用的任何单元的代用品 。与驱动程序一样 ,如果存根程序将数据返回到待测单元 ,它们也会通过 “压力测试”和适当的标称数据值 。驱动程序和存根程序的接口(包括它们的名称)均与真实单元的接口相同 ,从而可以在不改变被测单元的情况下连接单元组 。

单元等级的结构测试可以在实际的目标硬件 、实际硬件的仿真器或模拟器或者完全不同的处理器(如果情况要求)上进行 。例如 ,如果实际硬件尚未准备好决定单元测试的结果 ,但其中的代码却用更高阶语言写入 ,则可能会出现后一 种情况 。 因此在目标逻辑解算器不能支持测试的情况下 ,可以将高阶 AP编译并链接到另一个支持读取测试结果的逻辑解算器上 。

结构测试(也称为白盒测试)是通过被测项 目 (在这种情况下是单元) 在内部被查看 , 以确定该项目如何表现— 例如 ,确定所有可能的代码分支 。单元级结构测试的主要 目 的是验证 AP符合设计 ,包括逻辑 、算法的正确性和准确性(与并行 AP或手工计算相比) , 以及数据的工程单元的正确性 。这需要对每个单元进行完整的分支测试 、完整的 AP测试(包括确认没有死代码)和压力测试(例如检测溢出条件以及标称和最大循环控制数据值) 。详细设计用于制定验收标准 。

—集成等级和系统等级结构测试的环境

最好是用实际硬件和在一定程度上切实可行的环境设置集成和系统结构测试 。有几个原因 , 但其中两个最重要的原因是 : (a) AP可能既有 一 些好的也有 一 些坏的敏感条件 , 这些条件只有在实际硬件中运行时才显露出来 ,而且(b) 宜在硬件上确认最终 SIS(包括预期硬件和 AP)的运行情况 ,结构测试宜推动 AP开发朝着这一 目标前进 。然而 ,在模拟环境中进行部分或全部结构测试也是有充分理由的 。在考虑建立模拟能力时 ,最常用的两种配置是既仿真逻辑解算器同时模拟环境 ,或者既模拟逻辑解算器又模拟环境 。在使用环境模拟和有时使用逻辑解算器时 ,主要的优点包括 :

- 具有设置绝对已知输入值的能力 ,这样就可以预先确定结果 ,为每个测试建立验收准则 ;

- 模拟器可以很容易地建立超过 、低于和处于关键数据值精确限值的输入;
- 易于设置非法输入，以便测试所有的错误和失效条件;
- 可以很容易地看到每个测试的结果 。

—集成等级结构测试

集成结构测试通过编译和/或组装和连接这些部件，以及所需的驱动程序和存根程序 ,将经过验证的 AP部件(包括经过单元级结构测试的 AP部件)的功能性内聚单元组合起来 。然后将结构加载到实际或模拟环境中执行 。这允许测试人员关注 一 个功能包来确认其正确的操作，包括所有的内部和外部接 口 。在每个功能包的测试完成后 ,下一个功能包可以单独测试 ,或者添加到以前测试的包中(即与之链接) 。需在以前测试的软件包上执行回归测试(即运行以前成功运行的测试用例的选定子集)，以确保它们不会受到新引入的功能包的不利影响 。

—增量式方法

集成等级结构测试的增量式方法是 AP开发人员(与第三方 、确认测试人员相对— 见下文)使用的最好方法 ,特别是在 AP较大或复杂的情况下 。在这一方法中 ,对已选定的功能内聚小部分 AP进行编译 、连接和测试 。这一方法的使用无关 AP生命周期开发方法 ,包括以下三种方法中的其中任何一个 。在瀑布法中 ,先制定所有的要求 ,然后完成设计 ,最后对所选择的“思路”进行编码 ,并进行结构性的测试 。在螺旋法中 ,对 AP系统的主要装置进行讨论 ,然后制定要求 、设计和代码 ,在继续讨论和开发下一个主要装置之前 ,执行装置的结构测试 。最后 ,在增量 AP开发法中 ,可制定所有的规范和要求 ,但一次只设计和实现一个功能 。

在任何情况下 ,如果为被测系统开发专门的操作系统 ,则首先宜对这一操作系统进行结构性的测试 。如果这一部分的代码本身较大和/或复杂 ,宜将其分解成多个功能内聚包;否则 ,可将它作为一个实体进行结构测试 。需要测试的第二部分 AP通常是专门的输入/输出部分 。 如果有多样化的输入/输出装置 ,则可能需要单独对这些装置进行结构测试 。通常最好选择一条包括输入数据和可查看每次结构测试结果的思路 。第三步是选择应用和需要支持该应用的公用设施的功能内聚部分 ,并进行结构测试 。然后 ,选择 AP的下一个功能内聚部分以及用于下 一个结构测试的相关应用公用设施等等，以此类推 。需视情况对之前测试过的所有功能进行回归测试 。

在审核过程中 ,宜验证 AP中数据格式的以下方面：

- 完整性(例如，已经实现了所有的安全功能 ,并且已经考虑了每个安全功能的所有状态)；
- 自我一致性(例如 ,在整个程序中，已经采用了相同的 一 致性 ,并确保安全逻辑是清晰的，能 自我解释 ,并与非 SIF逻辑如状态报告等在视觉上隔开)；
- 防止未授权更改(例如宜使用两级保护 ,一级位于应用编程站内，以确保应用源代码在未获得适当授权的情况下不得修改 ,第二级用于确保某一 AP在未获得适当授权的情况下不能被下载到 SIS中)；
- 与功能要求的一致性(例如 ,确保已经正确解读了每个功能要求)；
- 与数据结构的一致性(例如 ,确保数据结构是可读的 ,并确保在整个 AP中使用相同的格式)；
- 与底层嵌入式软件的兼容性(例如 ,执行顺序 ,运行时间)；
- 正确的数据值(例如，已经使用了正确的数据类型 ,如整数或浮点 、布尔值等)；
- 在已知的安全界限内运行(例如 ,在应用内进行范围检查，以便确保这些值处于预计和测试范围内)；
- 具有安全修改的能力 。

还宜验证 AP, 以确保对可修改参数提供保护 ,避免出现：

- 无效或不明确的初始值(例如 ,确保可输入的所有可修改值都有默认值，以保证用户未输入任何值时使 AP保留在适当的范围中)；

- 错误值(例如,当某一个值超出测试范围或过程预计范围时,发出警报或关机);
- 未授权变更(例如,确保用户不能做出未授权变更或者某 一个值不能由于另 一 系统内发生故障而改变);
- 数据损坏(例如,确保数据不会被任何非安全任务或系统损坏)。

宜验证通信 、过程接口和相关 AP是否进行了失效检测,并执行避免信息损坏的数据确认,除非通过符合 IEC 61508要求的装置进行处理 。

对所有的安全功能来说,宜检查应用响应时间,以确保通过该应用的数据路线可以满足过程安全时间的要求 。例如,逻辑布局可能表示 AP宜在安全功能动作之前执行过几个循环 。

A.12.5.4 未提供进一 步指南 。

A.12.5.5 从正式测试开始,宜严格按照规定的修改程序实现 AP功能和配置数据的所有变更 。

A.12.5.6 未提供进一 步指南 。

A.12.6 “应用程序方法和工具的要求”指南

A.12.6.1 关于进一 步指南,见 GB/T 20438.3— 2017的附录 D 和 ISA TR 84.00.09。关于附加考虑,还请参阅附录 G。程序员不得在安全手册规定的范围之外进行任何假设,例如,使用安全手册中忽略的编译器能力 。理想情况下,编译器宜被配置为强制执行这些限制 。

对于某些 PE系统来说,配置功能的全部范围包括难以证明并通常以可预测方式响应的算法有关的一般控制功能— 例如,利用不会可靠终止的算法(例如,递归)或在程序执行中产生例外情况的算法(例如,“tan90°”)。对于这种类型的系统来说,制造商通常会提供一 份“PE手册”,其中规定了哪些功能可用于安全应用 。此外,在使用 一 般用途 PE系统的情况下,可能需要限制工具使用的方式,从而避免已知的工具在其运行过程中出现故障(通常这可以在用户讨论论坛上找到),并将编程功能的复杂性限制在那些已被证明行为可靠的功能上 。在这种情况下,有必要提供 PE手册并增加附加流程,以限制使用这些工具的方式(例如,指定良好的编程实践),识别任何不安全的特性(例如,未定义的语言特性,非终止算法),识别检查以发现配置中的错误,并指定记录 AP 的程序,以确保 AP 的可预测性 。如果 PE手册中未定义 SIS的架构,则这些流程还宜包括处理故障裕度的方式,例如冗余和多样性 。宜考虑是否定义额外的 AP约束条件(如看门狗 、数据检查等)。

还可将使一组程序员生成类似格式和风格程序的说明和示例作为安全手册的一部分或特定应用文件提供 。这些说明宜包括程序中尚未使用的特定算法或功能的详细情况,因为这些算法或功能可产生也许会影响安全性的意外行为 。

PE安全手册的典型章节为 :

a) 适用于哪种设备或系统的安全完整性等级;
b) 每个库功能的预期行为(即保证所使用编程语言的清晰句法和语义);
c) 旨在限制应用语言和工具箱“不安全”特征使用的规则和约束条件;
d) 工具和编程语言的要求和限制条件;
e) 嵌入式看门狗的使用;
f) 程序员如何用编程工具检查数据变量正确使用的指南 。需要提出的其他特征可能包括内存映射 、状态标识检查和输入值的有效性检查 。

A.12.6.2 宜确定一组用于开发 AP的方法和技巧,并判定其选择的合理性 。

E.1中给出了支持应用编程的典型工具箱 。

宜选择一些方法和技巧来将开发过程中引入 AP的风险降至最低 。这可能包括以下方面的考虑 :

- 清晰的句法和语义;
- 应用的适用性;
- 系统开发 、维护和使用过程所涉及人员的可理解性;

- 对 SIF非常重要的特性保证(例如最糟糕的用例执行时间)；
- 在类似应用中成功使用的证据；
- 旨在限制该方法“不安全”特征使用的规则和约束条件—关于进一 步指南 ,见 E. 2 和 E. 3;
- 数据条目执行和更新的确定性次序 。

用于消除故障的方法和技巧包括审核、模拟测试、分析和分析证明—另请参阅 GB/T 21109. 1— 2022 的 12. 5。

为了确保留在 AP 中的故障不会导致不可接受的结果 ,可以考虑以下方面：

- 在线检查技巧和例外情况处理；
- 供应商离线数据库和全局故障报告的使用；
- SIS失效报告和过程问题的监测以及它们对 SIS 的影响；
- 关键的 SIS功能在其他系统中的镜像；
- SIS AP 副本在培训过程中的使用 。

用于管理修改的方法和工具包括配置和版本控制 、要求管理数据库 、竣工文件的更新 、文件控制和变更管理 、变更责任的可追溯性和跟踪 、自动测试套件 。

为了实现这些方法和技巧 ,宜选择多个工具 ,从而降低它们在实际应用中的人为错误 。这可能包括以下方面的考虑：

- 由开发小组的合适成员熟悉工具；
- 在类似应用中成功使用这些工具的证据；
- 旨在限制这些工具“不安全”特征使用的规则和约束条件；
- 所有工具和 SIS精确版本的文档化记录；
- 不同工具之间以及与 SIS 的兼容性；
- 生成 AP文件的能力；
- SIS子系统行为的可预测性；
- 在 AP设计与硬件之间故障裕度架构的兼容性 。

PE应用开发环境和语言宜符合 GB/T 20438. 3— 2017 的表 A. 3 的要求 。

在决定使用未作为 PE 系统一部分提供的工具的情况下 ,宜考虑如何达到以下属性：

- AP安排的简单性；
- 在 AP 中提供注释 ,解释其功能和预期行为；
- 如何最大化和证明测试覆盖率；
- 对 SIF重要的属性的保证(例如 ,最坏情况的执行时间)；
- 合适的说明和自然语言支持；
- 反应该应用的划分；
- 与其他相关 AP 的风格共性 。

其他可以考虑的方法 、技术和工具包括度量(例如 ,测试覆盖率)和使用不同的工具来增强功能的验证(例如 ,背靠背工具) 。

需考虑工具(不一定是在最初系统开发过程中使用的那些工具)在 SIS 的整个寿命期内提供相关服务的可用性 。

A. 12. 6. 3 关于编程环境和工具特性的进一 步详细说明 ,见附录 E。

A. 13 工厂验收测试(FAT)

A. 13. 1 目的

工厂验收测试(通常包括 AP集成测试)的 目 的是 ,表明 SIS 可以在要求的响应时间内实现所有要

求的 SIF,满足 SRS的其他功能要求 ,并且没有可任何预测的不良行为 。

A. 13. 2 “建议”指南

A. 13. 2. 1 宜对用来实现那些具有相当复杂的应用逻辑或者冗余安排(例如，1oo2、1oo2D、2oo3等) 的安全仪表功能的逻辑解算器仍需进行一次 FAT。

A. 13. 2. 2 FAT最重要的部分是要有一个定义清晰 、编写优良和结构优良的测试规程 ,此规程定义了怎样测试应用逻辑以及在每一 步骤之后需查看的内容 。

操作过程的人员宜参加 FAT, 因为此测试会对他们进行操作 SIS的某些初步培训 。通常 ,他们也会对测试过程提出一些好的建议和提高方案 ,而这些方案一般在设计阶段没有被预见到 。

A. 13. 2. 3 未提供进一 步指南 。

A. 13. 2. 4 未提供进一 步指南 。

A. 13. 2. 5 在 FAT期间 ,宜测试接口(例如 ,BPCS和 SIS之间的通信接 口) 。

A. 13. 2. 6 未提供进一 步指南 。

A. 13. 2. 7 未提供进一 步指南 。

A. 14 SIS安装和调试

A. 14. 1 目的

未提供进一 步指南 。

A. 14. 2 “要求”指南

A. 14. 2. 1 未提供进一 步指南 。

A. 14. 2. 2 宜按设计和安装计划安装 SIS。宜与项目组正确审查 SIS与设计的任何偏离，以确保仍能满足所有的设计要求 。在正确安装 SIS之后 ,宜对 SIS进行充分地调试 ,并启动确认活动 。

A. 14. 2. 3 尽管 GB/T 21109. 1— 2022已把调试作为 一个单独的阶段进行了论述 ,但要认识到应用 、项目组经验以及项目需求可能要求调试分几个阶段来完成 。 仪表配置包括那些确保该仪表根据 SRS或安全手册正确运行的设置(例如 ,衰减 、线性化等) 。

A. 14. 2. 4 宜生成表明符合要求配置的文件(即符合 SRS或安全手册的要求) 。

A. 14. 2. 5 未提供进一 步指南 。

A. 15 SIS安全确认

A. 15. 1 目的

SIS安全确认的目的是确认 SIS能达到安全要求规范中所描述的要求 。宜在 SIS投入运行之前完成确认活动 。

A. 15. 2 “要求”指南

A. 15. 2. 1 未提供进一 步指南 。

A. 15. 2. 2 AP确认计划宜作为整体 SIS或 SIS子系统确认计划的一部分 。

A. 15. 2. 3 未提供进一 步指南 。

A. 15. 2. 4 如果 SIS已通过 FAT,那么在确认过程中 ,这可能需被考虑 。确认组宜审查 FAT 的结果，以确保成功地测试了全部 AP,并且纠正了 FAT过程中发现的所有问题 。

确保不存在装运/存放/处理损伤 、确保所有传感器和最终元件已被正确地连接到逻辑解算器上 、确保正确执行了仪表安全功能，以及确保操作员接口能提供必要的信息是非常重要的 。

A. 15. 2. 5　未提供进一 步指南 。

A. 15. 2. 6　测试的最终阶段(即用预期物理装置和接口以及规定的操作规程证实集成系统在它的预期环境中正确运行)只能在完成整个系统安装后以及在调试过程中才能彻底完成 。

A. 15. 2. 7　未提供进一 步指南 。

A. 15. 2. 8　在 PE SIS中 ,输入和输出的强制不得用作 AP操作规程的一部分 。

除非工厂批准的程序和访问安保措施予以补充 ,否则不允许在不停止服务的情况下强制输入和输出 。任何这样的强制行为都需被通告或者触发警报 ,视情况而定 。

对维护时设置的超驰/旁路都宜给出适当的通告 。

A. 16　SIS操作和维护

A. 16. 1　目的

未提供进一 步指南 。

A. 16. 2　“要求”指南

A. 16. 2. 1　宜建立一个 SIS维护计划 。该维护计划宜描述由 SIS失效或维护导致的 SIS的所有潜在降级模式 。宜识别与这些降级模式有关的补偿措施 ,并制定维护计划 。宜记录所有的维护动作 。

A. 16. 2. 2　在过程运行中如果某一 SIF出现失效和/或旁路 ,则出现不安全过程状态的可能性会增大 。因此 ,宜制订以下程序 :

- 诊断失效情况 ,特别是失效模型 ,制订相关风险降低措施;向操作员发出警报;
- 确定补偿措施 ,从而可以在可容忍的安全等级中持续运行;

注　1: 测试诊断程序的一个例子是插入人为故障 。

注　2: 失效模式和影响分析是用于风险分析的重要工具 ,建议使用这些工具 。

- 由于功能检验测试造成的旁路 。

严格的操作规程和风险缓解措施适用于旁路的启动和解除(例如 ,应用旁路之前的审批 、当旁路就位时向操作员发出警报 、在返回到完全操作状态之前进行回路检查) 。宜对操作员进行适当的培训 。

用于测试诊断程序的方法和规程 。 如果采用了故障插入测试 ,则宜考虑负面影响 ,以确保系统的 SIF和 SIL在返回到完全操作状态后仍然能满足功能安全要求 。

如果诊断通过故障插入测试表明故障 ,则宜进行适当的分析 ,以确定故障对 SIF及其 SIL 的原因和影响 ,并采取以下行动 :

- 根据维护规程处理随机硬件失效(例如 ,维护或变更该设备);或者
- 返回到相关的生命周期阶段 ,并根据变更过程的管理继续处理系统失效(例如 ,未检测出来的设计错误) 。

A. 16. 2. 3　可对以下方面进行说明 。

- 要求采用补偿措施的需求原因 。
- 补偿措施的使用说明 。
- 补偿行动将采取哪种方式将过程带到安全状态 ,响应时间和补偿措施故障的后果 。
- 宜对启动和解除旁路采用严格的操作程序和风险缓解措施(例如 ,在施加旁路前批准 、在旁路已经设置时向操作人员发出警告 、在完全恢复运行前进行回路检查) 。宜为操作员提供适当的培训 。

A. 16. 2. 4　未提供进一 步指南 。

A. 16. 2. 5　未提供进一 步指南 。

A. 16. 2. 6　未提供进一 步指南 。

A. 16. 2. 7　未提供进一 步指南 。

A. 16. 2. 8　未提供进一 步指南 。

A. 16. 2. 9　未提供进一 步指南 。

A. 16. 2. 10　未提供进一 步指南 。

A. 16. 2. 11　用于传感器和最终元件的检验测试规程宜包括充分测试工艺气体/液体的接 口 。通过远程访问进行的测试会影响 SIF的执行 。

注 ：使用本地智能设备时 ,可以执行在线测试 。

A. 16. 2. 12　未提供进一 步指南 。

A. 16. 2. 13　在 SIL确定过程中所做的假设可能会影响系统的 SIL。

操作管理宜审核和验证 SIL确定过程中所做的假设 ,包括占用情况 、回避概率 、避免或降低要求的规程以及报警规程 。

如果这些假设与实际情况不符 ,则宜进行新的风险分析 。

A. 16. 3　检验测试及检查

A. 16. 3. 1　“检验测试”指南

A. 16. 3. 1. 1　宜选择检验测试间隔以达到安全要求规范中规定的要求时的平均失效概率 。

A. 16. 3. 1. 2　SIS的检验测试需要尽可能准确地反映真实的操作条件 。　检验测试宜在任何可能使代表性测试结果失真的定期维护活动之前执行 。

SIS的检验测试更适宜作为整体测试来执行 ，即宜对整个 SIS回路同时测试 。　检验测试可作为端对端(即全回路)集成测试来执行 ,也可采用分段的方法(一 系列有交叠的设备级测试 ，即传感器 、逻辑解算器和最终元件)来执行 。检验测试宜包括但不限于以下条件的验证 ：

a)　操作逻辑顺序 ,例如因果图中给出的操作逻辑顺序;

b)　所有输入设备(包括现场传感器和 SIS输入模块)的操作;

c)　与每个输入设备相关的逻辑;

d)　与组合式输入有关的逻辑;

e)　所有输入的跳闸触发值(设定点) ;

f)　报警功能;

g)　SIS的响应速度(必要时) ;

h)　SIS输出模块和所有最终元件的操作;

i)　由 SIS执行的计算功能;

j)　输出设备的时序和速度;

k)　人工操作的功能使过程进入安全状态;

l)　用户启动诊断程序的运行;

m)　SIS在测试之后仍然是运行的 ,例如 ,任何抑制或超驰的复位 。

如果由于安全或操作原因而不能进行 SIS的整个回路测试 ,则可以为 SIS回路的设备或子系统部分执行一部分测试 。某些项目可在过程运行条件下通过提供输入信号的抑制或输出动作的超驰而进行测试 。　因此 ,造成过程关闭的项目如工艺阀可在计划好的停车期间内进行测试 。

对于采用部分测试的那些应用而言 ,宜编写测试规程 ，以确保所有回路项目都包含其中 ：

- 在单元装置关闭时测试最终元件;
- 在线测试时 ,尽可能通过实际可及的输出设备(例如 ,输出跳闸继电器 、关断电磁阀 、部分阀门行程运动)对 SIS进行测试;
- 在计算 SIF的 PFD_{avg}时 ,宜考虑最终元件测试周期的限制条件 。

宜对冗余架构的所有路径进行检验测试 ，以证实所有的通道都在正确地运行 ,而不仅仅是足够的通

道启动输出 。这通常要求做好专门的准备，以便于测试 。

在预先确定的间隔中 ,宜执行完整的 SIS回路测试 。

未包括在这些测试中的部件宜通过其他方式来证明，例如，如果不能通过检验测试检测出危险失效 ,则宜在预先确定的间隔中检修这一项 目 。

对于阀门 ,部分冲程测试可以被视为功能测试 ,涵盖 一 部分可能的故障，而不是诊断覆盖的 自我测试 。检测到的部分宜通过故障模式 、影响和诊断分析(FMEDA)或类似的方法正确记录 。

A. 16. 3. 1. 3　检验测试频率宜符合应用厂商的建议和良好工程惯例;如果根据以往操作经验认为有必要 ,也可以使用更高的测试频率 。

有许多策略可用于选择 SIF的检验测试间隔 。

例如 ,有些用户选择尽可能长的检验测试间隔，以使维护成本最低和使测试的潜在影响最小 。在这种情况下 ,SIS设计可能在装备上包括更多的冗余 ,增加诊断覆盖率和鲁棒性 。在设计完成之后 ,则可对设计进行一次计算 ,从而确定能达到 SIF定义的 SIL性能的最大测试间隔 。这种设计理念的负面影响会导致工厂中的每个系统都有不同的测试间隔 ,并可能要求更严格的适应性跟踪 。这种设计理念也可能鼓励设计性能趋向性能曲线的下端(例如对 SIL1的系统 ,$PFD_{avg}=10^{-1}$;对 SIL2的系统 ,$PFD_{avg}=10^{-2}$) 。

宜注意 ,PFD_{avg}是 一个与时间相关的概率，当时间增加时 ,它也会增加 。 因此对于较大的验证测试间隔来说，即使在通常达到 SIL 目标的情况下 ,它可能会变得非常大 ,而且它可能会变成非常糟糕的风险指标 。这可能是不可接受的 ,但在某种程度上 ,错开测试降低了这一 问题的影响 。

其他用户可能希望根据已定义的检验测试间隔进行标准化 ,并以同样的测试间隔对工厂的所有系统进行测试 。例如 ,它们可能希望每年测试每个 SIF,从而它们就可以相应地设计每个 SIS。在开始设计之前 ,预选一个检验测试间隔 ,用户就可预选能满足大多数应用要求的 SIL的结构 、设备和诊断覆盖率 。通过把这种设计定义在公司标准中，可以降低大多数应用的设计工程成本 。 在这种情况下，宜对SIS进行一次计算，以确保使用预选的检验测试间隔可以满足所要求的 SIL性能 。

此外 ,在诸如以下给定条件下，由于在运行过程中对 SIS的实际要求而造成的停车可被认为是检验测试(完整或部分测试)：

- 停车记录了与对应检验测试中等效的信息;
- 停车包括 SIS的所有部分 ,宜单独测试未激活的设备或 SIS子系统;
- 停车发生在进行下一次计划的检验测试前预定的最大时间窗内(由此该计划的检验测试可取消) 。

如果满足这些条件 ,则可跳过下一次计划的检验测试 。

在选择一个检验测试间隔时 ,宜对要求模式系统的要求率 、每个被测设备的失效率 、整个系统性能要求进行考虑 。

A. 16. 3. 1. 4　未提供进一 步指南 。

A. 16. 3. 1. 5　未提供进一 步指南 。

A. 16. 3. 1. 6　未提供进一 步指南 。

A. 16. 3. 1. 7　未提供进一 步指南 。

A. 16. 3. 2　“检查”指南

如 GB/T 21109. 1— 2022所述 ,检查 SIS不同于检验测试 。尽管检验测试可确保 SIS运转正常 ,但都需要通过目视检查来确认安装的机械完整性 。

通常是在检验测试的同时进行检查 ,但在需要时也可更频繁地进行检查 。

注 1: 检查可能会检测到早期失效 ,而检验测试则不能发现这些失效 。

注 2: 在较差的条件中 ,某 一 SIS元件 、子系统或系统的失效率(λ)可能会高于 PFD_{avg}和残余风险计算中假定的失效率 。任何此类项目的较差条件均可补救 。

A.16.3.3 “检验测试和检查的文档”指南

对在检验测试和检查结果中的所见记录进行归档是重要的 。关于这些结果要保存多久没有特别要求,不过为了能复查以往结果,以便查看设备是否存在失效历史,通常宜保存足够长的时间 。

例如,如果一个传感器未能通过检验测试,最好是检查以前的检验测试结果,看看这个传感器在过去几次测试中是否也未能通过类似的检验测试 。如果历史记录显示重复故障,宜考虑使用不同类型的传感器重新设计 SIS。

A.17 SIS变更

A.17.1 目的

变更主要适用于在 SIS的操作阶段中出现更改 。

A.17.2 “要求”指南

A.17.2.1 SIS(子系统或元件)的每次改变就是一 次变更,除非执行同样的实物更换 。此类变更可能包括与以下方面有关的问题：

- 新的检验测试间隔或程序；
- 具有不同特性的元件,例如更换过时的元件；
- 设定值的变更；
- 操作条件的改变；
- 操作程序的改变；
- 应用软件或固件的变化；
- 系统性失效的纠正；
- 失效率高于预期；
- 要求率升高 。

A.17.2.2 未提供进一 步指南 。

A.17.2.3 只要有可能,宜避免对 SISAP进行在线修改 。如果要求进行在线修改,则整个规程宜文档化,并根据安全计划进行审批 。

A.17.2.4 未提供进一 步指南 。

A.17.2.5 未提供进一 步指南 。

A.17.2.6 未提供进一 步指南 。

A.17.2.7 未提供进一 步指南 。

A.17.2.8 未提供进一 步指南 。

A.18 SIS停用

A.18.1 目的

未提供进一 步指南 。

A.18.2 “要求”指南

A.18.2.1 未提供进一 步指南 。

A.18.2.2 未提供进一 步指南 。

A.18.2.3 未提供进一步指南。
A.18.2.4 未提供进一步指南。
A.18.2.5 未提供进一步指南。

A.19 信息和文档要求

A.19.1 目的

关于文档结构的例子,见 GB/T 20438.1— 2017的附录 A,更多详情,见 IEC 61506。文档可以通过不同的形式获得(例如,纸质文档、需要在屏幕或显示器上呈现的胶片或任何数据媒介)。 附录中给出了各种各样不同的文档例子。

A.19.2 “要求”指南

A.19.2.1 可用来实现一个 SIS的信息和文档清单包括:

a) H&RA 的结果,
b) 保护层分配,
c) 在确定完整性要求时使用的假设,
d) 安全要求规范,
e) 应用逻辑,
f) 设计文档,
g) 变更信息和/或文档,
h) 验证和确认的记录,
i) 调试和 SIS确认规程,
j) SIS操作规程,
k) SIS维护规程,
l) 检验测试规程,
m) 评估和审核结果。

A.19.2.2 SIS宜按照能清楚地将其从其他非安全相关系统如BPCS中区分出来的方式来识别和文档化。
A.19.2.3 未提供进一步指南。
A.19.2.4 未提供进一步指南。
A.19.2.5 未提供进一步指南。
A.19.2.6 未提供进一步指南。
A.19.2.7 未提供进一步指南。
A.19.2.8 关于含有 SIS设计的典型文件清单,见 F.26。
A.19.2.9 未提供进一步指南。

附 录 B
（资料性）
使用可靠性框图开发 SIS逻辑解算器应用程序的示例

B. 1 概述

下面的示例将描述：

- 组织符合 GB/T 21109. 1— 2022的 6. 3要求的 AP开发相关活动的方法;
- 依据 SRS生成 APSRS,从而符合 GB/T 21109. 1— 2022的 10. 3. 2 的要求;
- AP中两个关机功能的开发和实现,符合 GB/T 21109. 1— 2022的 7. 2. 2、11. 5. 2. 3、12. 1、12. 2、12. 3、12. 4、12. 5、12. 6和15. 2. 2的要求。

B. 2 应用程序开发和确认原理

为了帮助 AP工程师设计具有可预测性能和要求安全完整性的 SIF(即 SIL3),需要采用 一 种高效的开发方法 。

传统上,在设计工作后期，当实际的硬件架构可用时，AP设计工程师方可进行 AP设计的完整测试 。这是一种效率非常低的方法，因为在这一 阶段发现错误时,他们需要回到相关的设计阶段纠正错误并生成一个新版本,从而导致在开发最终产品的过程中时间和费用大幅增加 。

在处理 SIF规范中常见的高级 、复杂的安全要求时,传统的基于文本形式的 AP规范不具备足够高的效率 。

针对这些挑战而采用的最高效工具是基于模型的设计(MBD) 。 MBD是说明与设计复杂安全系统相关问题的数学和直观的方法,这种方法被成功地应用于很多领域 。它给出了 一 种在安全生命周期的开发阶段克服很多困难的高效方法 。此方法和示例包括以下步骤：

— 通过以下方式对 APSRS建模 ：
  - 识别相关的 SIS元件 。
  - 用适当的建模语言描述它们的行为 。
— 分析及综合对 APSRS可预见的实现满足需求的行为;
—证实 AP实现与 SRS的符合性，以便用文件记录该确认过程,并有助于满足 GB/T 21109. 1— 2022的 12. 5 和第 15章的要求 。

这可以使得错误在早期 AP设计过程中得以定位和纠正,从而将 AP修改的时间和费用影响降至最低 。对于 AP升级和对于导出的带扩展能力的 AP开发二者来说,使用 MBD有利于实现设计复用 。MBD为所有的开发人员提供了一个共用设计环境,有利于 一 般通信 、数据分析以及不同开发小组之间的 AP验证 。

虽然文本规范和模拟已经使用了很长的时间,但它们的效率却非常低,不足以处理 SIF的高级和复杂特征，因为这些工具具有完全非图形化的性质,并且没有提供支持评估的数学证明 。 由于图形化工具的局限性，因此设计工程师曾经高度依赖于基于文本的传统编程和数学模型 。这也曾经是针对如何保证安全完整性重点关注的原因，因为在基于文本的程序中开发模型不仅困难和耗时，而且非常容易出错 。调试模型和纠正错误曾经是一个冗长乏味的过程 。在可以创建出最终的无故障模型之前,它需要很多的测试和错误用例，因为功能模型在模型的转化过程中通过各种各样的设计阶段经历了许多看不见的变更。 如今,通过使用专门的图形化建模工具(由符合 GB/T 21109. 1— 2022 并涵盖 GB/T 21109. 1— 2022的 6. 3. 1 的整个 AP安全生命周期的开发软件包提供支持),人们已经克服了这些挑战 。这使得可以在单个库中开发规范和实现,与人工技术相比,其好处是能以非常低的成本证明安全

完整性特性 。该示例的一般性 AP开发原理是遵循基于模型的工程实践 。

以下模型将按顺序实现 、逐步集成和使用，以支持设计和验证：

— 功能模型：

- 硬件功能架构模型，
- 硬件物理架构模型，
- AP功能架构模型，
- AP架构模型 。

— 安全特性模型：

- 时间特性，
- 安全完整性特性 。

— 检查模型 。

为了顺序地证实 AP符合 AP SRS,这些模型会被逐步地集成在一起 。

这些模型用于：

—作为功能规范和安全完整性详细规范的实体化进行设计 ：

— 自动编辑的 AP生成;

— 通过模型检查进行半自动测试，以便验证每个 AP模块是否符合其功能和安全规范的要求 。

B. 3 应用描述

B. 3. 1 概述

这个例子是基于 LNG工厂 SIS的一部分 。

B. 3. 2 过程描述

示例的过程是液化天然气终端的一部分 。该工厂的 目 的是接收来自船舶的 LNG,储存并备用，以便输入到天然气供应管网中 。

B. 3. 3 安全仪表功能

B. 3. 3. 1 概述

用于上述过程的 SIS包括 7个 SIL3 SIF和 64个 SIL2 SIF。这 一 示例关注的是 一 个 SIL3 SIF和一个 SIL2 SIF。下文给出的信息可作为 SRS的一部分考虑 ,并作为 AP SRS的输入 。

B. 3. 3. 2 SIF02. 01—LNG卸载急停

图 B. 1 描述了与此功能有关的过程部分 。

该 SIL2功能的目的是,假设在三个 LNG 罐的其中一个罐内检测到压力超高时将船舶与工厂隔离。

当通过压力开关在三个 LNG罐的任何一座内检测到压力超高时(图 B. 1上未显示传感器) ,将触发对功能的需求 。然后这一 功能关闭 3个阀门(XV1008、XV2008和 XV3008) 。在给定延迟时间后 ,如果仍然存在压力超高 ,则关闭另外两个阀门(XV1014和 XV2014) 。 即使压力超高信号消失 ,这些阀门也仍应处于关闭状态直至复位 。

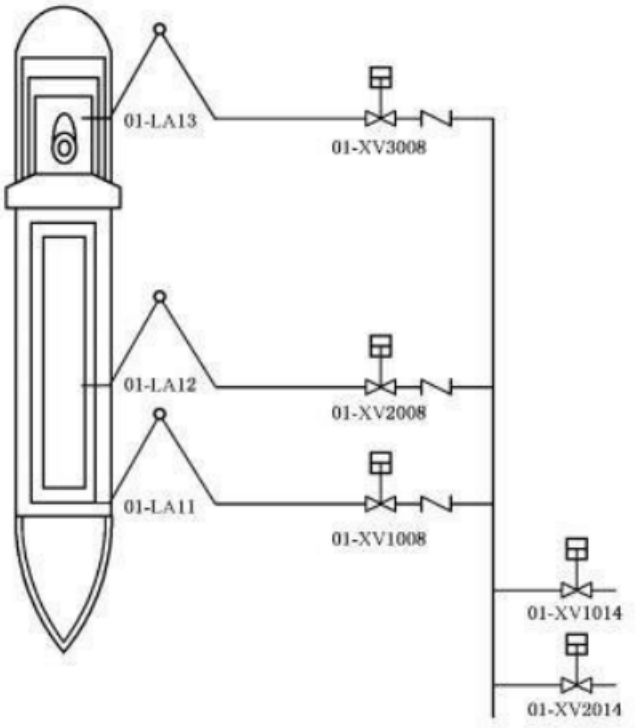


图 B.1 SIF02.01工艺流程图

B.3.3.3 SIF06.02—ORV进料阀的应急关闭

图 B.2描述了与此功能有关的过程部分 。

该 SIL3功能的目的是,在出口管上通过温度开关检测到温度超低时(图 B.2 中未显示传感器),通过关闭进料阀 XV1001和隔离阀 XV1013来隔离每个 ORV。为了不使气体滞留在阀门之间的管路中，每次应只关闭一个阀门 。在复位之前,即使超低温度信号消失,这些阀门也仍应处于关闭状态直至复位 。两个隔离阀都关闭会导致危险状态,避免出现这一危险状态的等级为 SIL2。

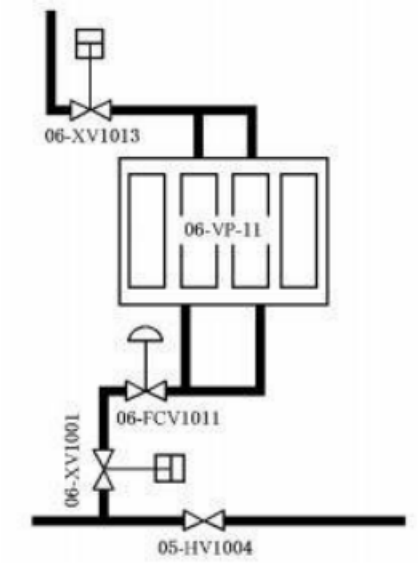


图 B.2 SIF06.02工艺流程图

B. 3. 4　风险降低和多米诺效应影响

风险分析表明对两个 SIF同时产生要求是危险的 ,不能发生 。

B. 4　应用程序安全生命周期执行

B. 4. 1　概述

本节按顺序描述如下：

- 从 SRS中提取的 APSRS开发所需的输入 ，
- APSRS开发(GB/T 21109. 1— 2022的 10. 3. 2) ，
- AP架构设计(GB/T 21109. 1— 2022的第 12章) ，
- AP建模 、设计和测试(GB/T 21109. 1— 2022的 12. 3 和 12. 4) ，
- AP集成建模和测试(GB/T 21109. 1— 2022的 12. 4 和 12. 5) ，
- AP生成 ，
- SIS确认的影响因素(GB/T 21109. 1— 2022的第 15章) 。

B. 4. 2　应用程序 SRS开发的输入

B. 4. 2. 1　概述

以下是来自前一个生命周期阶段的输入 。

B. 4. 2. 2　功能规范

图 B. 3 描述了从图 B. 1 和图 B. 2 中所述的要求细化得到的功能规范 。这些示意图描述了在决定未来必需的硬件及用于其实现的应用软件之前 SIF的预期行为 。

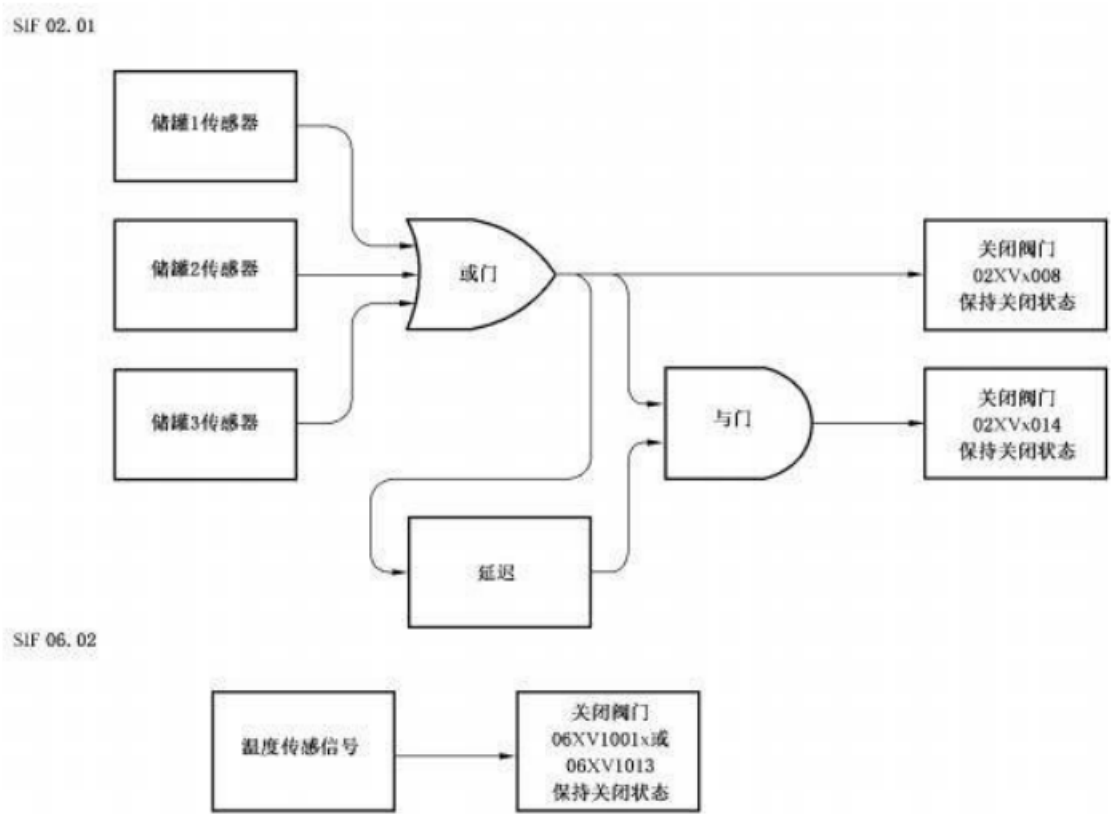


图 B. 3 SIF02.01和 SIF06.02的功能规范

B. 4. 2. 3 硬件功能架构

这些图表显示了在应用 HFT约束条件和 SRS其他要求之前实现 SIF所必需的硬件架构 。

图 B. 4 中说明了 SIF02. 01硬件功能架构 。

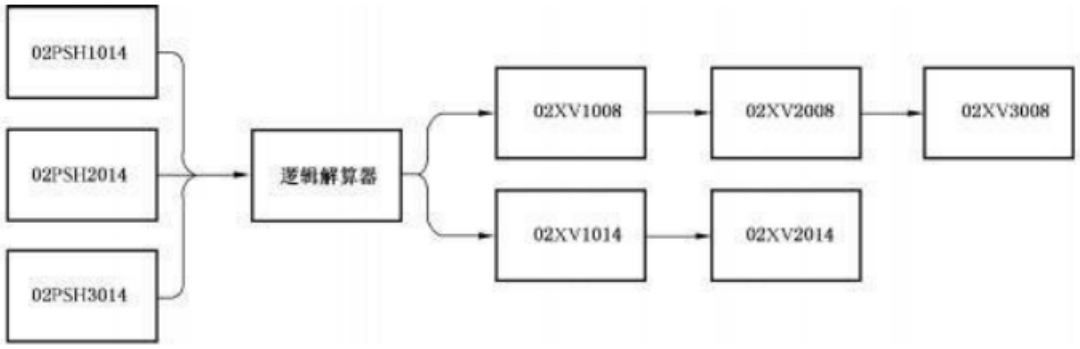


图 B. 4 SIF02.01硬件功能架构

图 B. 5 中说明了 SIF06. 02硬件功能架构 。

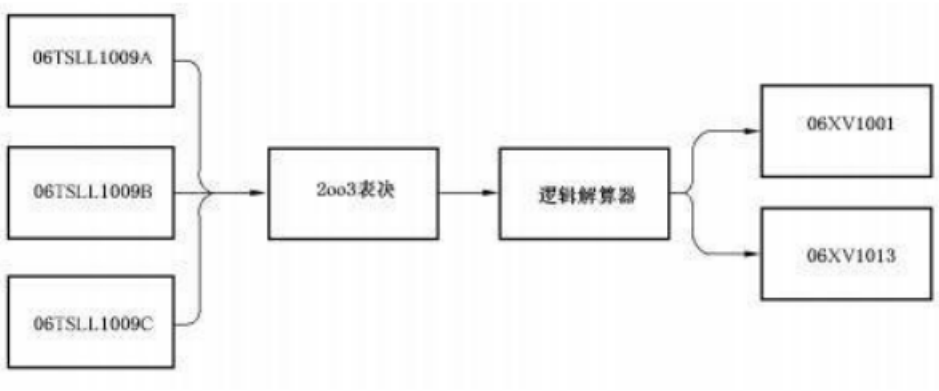


图 B. 5 SIF06.02硬件功能架构

B. 4. 2. 4 SOV/MOV 的硬件典型规范

管道和仪表图通常描述某一设备中所有的硬件和 AP接 口 。 图 B. 6 描述了同时在 BPCS和 SIS中的 SOV需要实现的硬件和 AP接 口 。

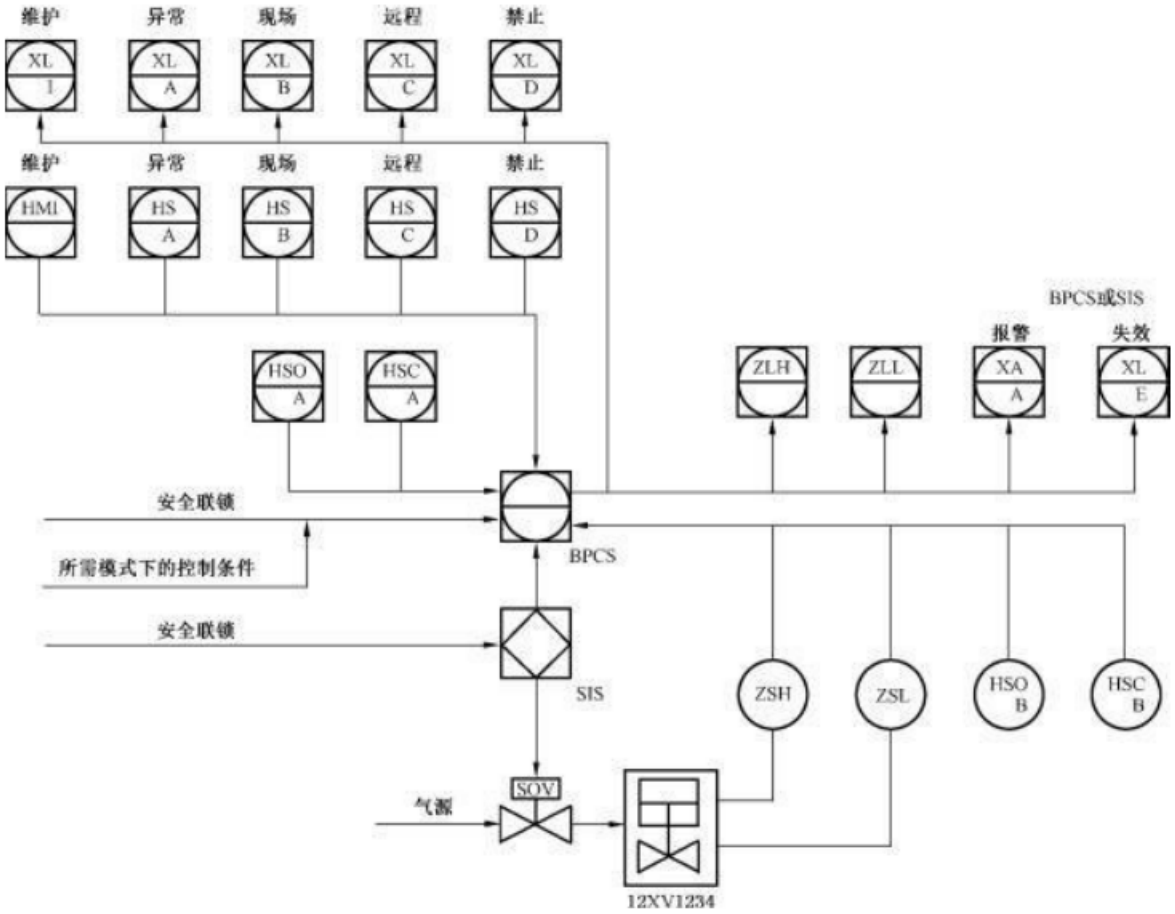


图 B. 6 从管道和仪表图中提取 SOV 的硬件规范

B. 4. 2. 5　硬件物理架构规范

对图 B. 5 和图 B. 6 中所描述的派生需求进行细化，可以得到所使用的实际硬件的定义，以及图 B. 7 和图 B. 8 中所描述的最终架构。

注 1: GB/T 21109. 1— 2022的第 11章要求中对硬件 HFT要求的应用的描述不在此讨论。

注 2: 在本例中，BPCS和 SIS之间的链接是离散的(硬接线)。

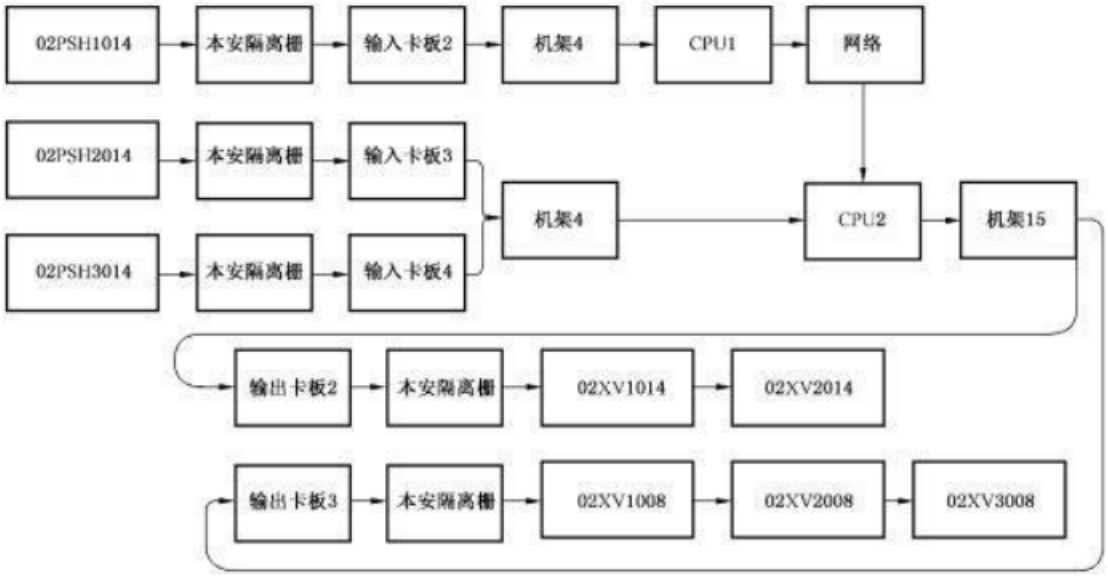


图 B. 7　SIF02.01硬件物理架构

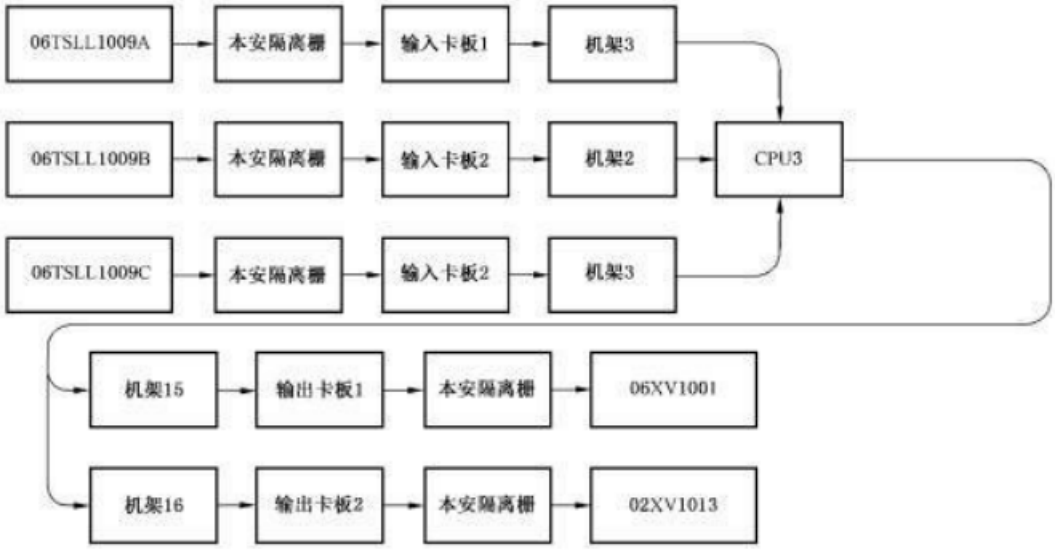


图 B. 8　SIF06.02硬件物理架构

B. 4. 3　应用程序设计和开发

B. 4. 3. 1　概述

B. 4子条款包括描述以下步骤的示例：

- APSRS开发，

- AP功能架构设计，
- AP功能设计 、建模和测试，
- AP集成建模和测试 。

B. 4. 3. 2 应用程序 SRS

B. 4. 3. 2. 1 概述

APSRS可组织如下 ：

— 与预期行为对应的功能要求：

- 设备(传感器和执行机构)的要求，
- 每个 SIF联锁的要求，
- SIF之间的联锁要求 。

—需避免的行为对应的安全完整性要求：

- 在设备层面，
- 在 SIF层面，
- 在更高的层面 ,如工厂级别 。

B. 4. 3. 2. 2 应用程序功能要求规范

B. 4. 3. 2. 2. 1 设备功能要求

设备的功能要求可根据设备类型来描述 ,并可组织如下：

—设备的一般操作模式;

—设备的功能规范 。

B. 4. 3. 2 提供了一个 SOV 的例子 。

执行机构的一般操作模式：

下文的表 B. 1定义了用于电磁操纵阀(SOV)操作模式的状态机 。

表 B. 1 操作模式规范

状态名称	描述
请求	当多个安全条件生成一个安全顺序时 ,要求根据更高等级的逻辑来控制阀门。这一要求的优先级高于任何其他的操作模式 。然后将设备锁定在要求模式内 ,从而使它的各个指令变得不可用，阀门只能由更高等级的逻辑控制 。 当该逻辑解除安全工况时 ,操作模式被强制变成 DISTANCE远程模式 ,然后操作人员可以 自 由地改变操作模式
远程	阀门通过 BPCS人机界面的打开和关闭指令控制 。这是初始状态
现场就地	阀门通过靠近阀门的本地按钮的打开和关闭指令控制
异常	只有当阀门已经位于安全位置时 ,才可能出现这一模式。所有本地和远程操作人员的指令变得不可用 。通过安全工况的控制仍然处于激活状态
维护	有当阀门已经位于安全位置时 ,才可能出现这一模式 。操作模式被强制变成故障状态 ,所有的报警均受到抑制

SOV功能规范 ：

该设备是一个隔离电磁操作阀,由 SIS和 BPCS控制 。

假设针对 SIF所保护的危险,SOV有唯一 的且不可变的安全位置 。此位置是关闭位置 。

SOV是一 台 自主的设备,它的各个指令来 自 BPCS,在特定情况下,它可由更高等级的逻辑控制 。控制某一设备如 SOV 的逻辑被称为 “典型逻辑” 。

此 SOV 的典型逻辑允许实现以下内容 ：

—来自 BPCS操作员站的打开和关闭指令 。

— 通过 BPCS,来自现场的本地打开和关闭指令 。

— SIS或 BPCS初始化时,进入安全位置 。

— SIS的打开和关闭命令 。

— 通过软件开关从 BPCS操作员站选择操作模式 。

— 重新排列以下情形的指令 ：

- 重新排列启动时关于限位开关信息的指令 ；
- 重新排列要求模式中关于更高等级逻辑联锁的指令 ；
- 重新排列现场模式中关于现场指令的指令 ；
- 重新排列安全动作情况中关于安全状态的指令 。

— 处理维护状态 。

—对两条限位开关信息中的阀门状态进行可视化处理 。

— 生成冲突警报(在打开或关闭时,同时检测限位开关 、限位开关失效) 。为了避免生成虚假的冲突警报,限位开关信息被延迟,从而使 SIS指令被传输到 BPCS中 。

— BPCS和 SIS失效检测 。

— 调谐和调谐参数修改 。

参数:冲突检测延迟 。

仅在维护级别访问 。

B.4.3.2.2.2 SIF功能要求

SRS中描述了每个安全功能的功能要求 。

B.4.3.2.2.3 SIF间联锁的功能要求

该层面中没有任何功能要求 。

B.4.3.2.3 安全完整性要求规范

B.4.3.2.3.1 设备完整性要求

设备完整性要求如下 ：

- 任何联锁组合不得阻止设备指令在要求时进入它的安全位置 ；
- 任何联锁组合延迟 SOV指令的时间不得大于 100ms;
- 任何联锁组合不得导致物理设备指令处于不确定或不稳定的状态 ；
- 状态机的所有过渡条件应是完整的,并具有排他性 ；
- 应确定状态机内每种工况的动作 。

B.4.3.2.3.2 SIF的完整性要求

SIF完整性要求如下 ：

- 当输入有效时,任何联锁组合不得妨碍功能向 SOV 的 AP典型逻辑提出某一请求；
- 任何联锁组合延迟 SOV请求的时间不得大于 100 ms;
- 任何联锁组合不得导致物理设备指令处于不确定或不安全的状态 。

B.4.3.2.3.3 SIF间联锁的完整性要求

SIF的完整性要求如下所述 ：

- 任何联锁或要求的组合不应导致对 SIF02.01和 SIF06.02同时提出要求 。

B.4.3.3 应用程序功能架构设计

B.4.3.3.1 架构设计

AP架构设计活动需确保 ：

- 所产生的架构将符合 GB/T 21109.1— 2022的 12.4.4的要求；
- 所产生的架构不得以任何方式使 SRS中所述硬件架构的系统性完整性降级 。

AP架构将基于层次化结构 。考虑以下层级和 AP模块 ：

- 多个设备的 AP典型逻辑:在这一示例中,我们将考虑电磁阀;压力和温度传感器 。这些模块包括与以下方面相关的逻辑:设备控制、输入获取和处理、标准的复杂功能如表决 。
- SIF逻辑:为了实现每个 SIF的预期行为而进行 AP模块的联锁 。
- 工厂逻辑:SIF联锁 。

这些 AP模块通过模型检查工作台环境中的图形化语言方式来描述,模型反映需要开发的 AP模块的预期行为 。所有的这些模块代表 SIF中需要产生的最终 AP,它们可被直接编译,并可下载到 目标逻辑解算器中 。

必需模块的列表(仅限于本例)是：

- SOV典型逻辑；
- 2oo3表决；
- 网络通信处理；
- 传感器处理；
- SIF02.01逻辑；
- SIF06.02逻辑 。

所有模块均根据图 B.9 中所述的结构集成在一起 。

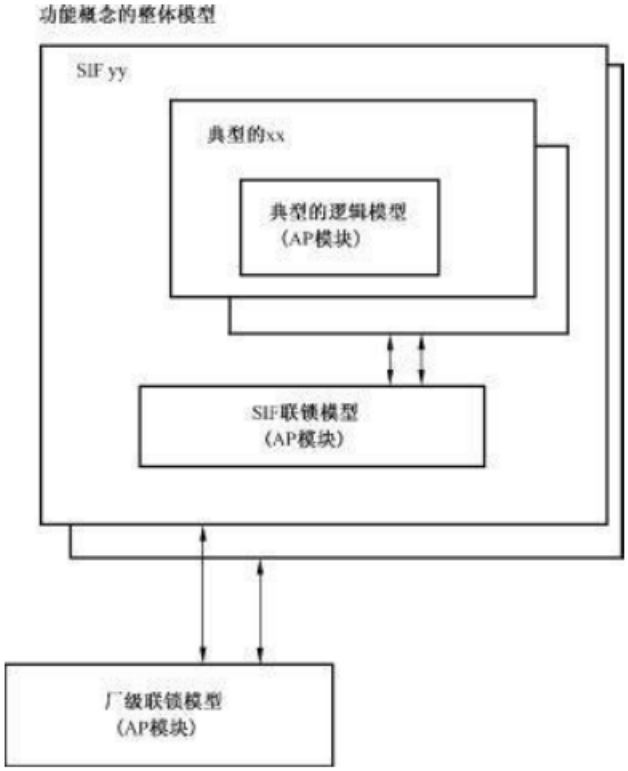


图 B.9 模型集成的层级结构

B.4.3.3.2 源自架构的安全完整性要求

B.4.3.3.2.1 概述

该架构不得以任何方式损害 B.4.3.3.1中定义的物理硬件架构的系统性安全完整性 。

这个问题在这里没有更广泛地讨论,因为它与选定逻辑解算器的特性直接相关 。但至少对于 SIF 02.01来说,有必要分析将 AP模块分布在 CPU1和 CPU2之间对 SIF系统性完整性的影响 。这将要求对硬件和 AP 的失效模式的组合进行分析 。这通常通过失效树的方式来完成,包括 AP模块的内部失效(与容纳 AP模块的硬件无关),旨在确定是否存在损害 HFT 的单点失效 。

此外,AP架构的定义使得可以确定需分配给每个 AP模块的派生 AP SRS。

B.4.3.3.2.2 设备的完整性要求

派生要求:

- 状态机的所有过渡条件应是完整的,并具有排他性;
- 应确定状态机每个条件的动作 。

B.4.3.3.2.3 安全仪表功能完整性要求

派生要求:

- 将 SIF联锁连接至相关模块的变量的动态值组合值不得导致某 一 SIF处于不确定或不稳定的状态。

注:这一要求并未重复 B.4.3.3.1的要求。B.4.3.3.1与逻辑的功能静态行为有关,而这一要求目前却与分布在2个 CPU 中的某一 逻辑的动态行为有关,并产生于架构设计 。

B. 4. 3. 3. 2. 4　工厂等级的完整性要求

无派生要求 。

B. 4. 3. 4　应用程序功能设计、建模和测试

B. 4. 3. 4. 1　应用程序模块的功能模型设计和测试

AP架构中确定的必要 AP模块需在模型检查工作台开发环境中建模 。　同时 ,构建模型以描述 :

- 物理设备的行为;
- 人机界面的行为;
- 设备所需的安全特性;
- SIF所需的安全特性;
- 工厂等级中所需的安全特性;
- 工厂的物理行为(通过工艺流体联锁) ;
- 逻辑的 BPCS部分 。

以上对于在功能和物理环境之前证明模型化 SIF的所需特性是必要的 。

根据图 B. 10中所述的结构 ,将所有的 AP模块在功能检查模型中集成在一起 。

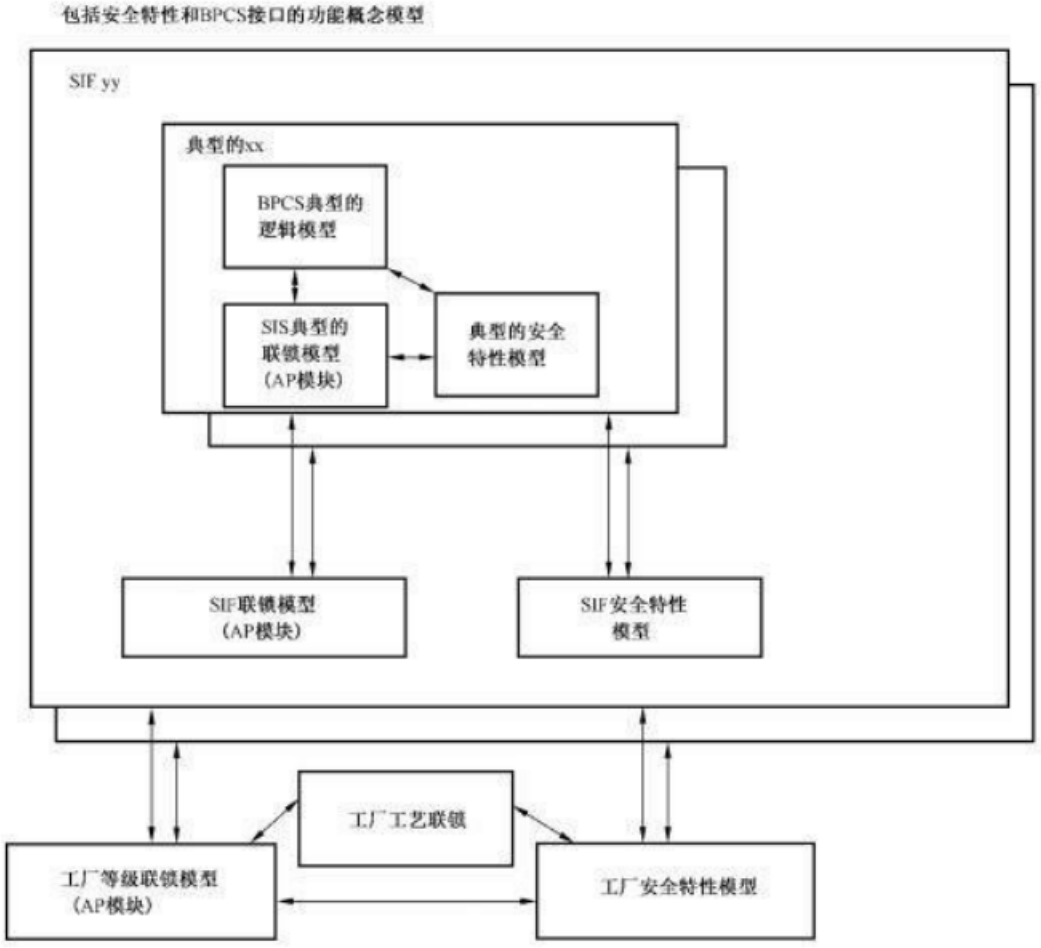


图　B. 10　包括安全特性模型和 BPCS逻辑模型的模型集成的层级结构

B. 4. 3. 4. 2 模型描述

B. 4. 3. 4. 2. 1 应用程序典型逻辑层面

SOV BPCS控制逻辑模型：

表 B. 1要求中操作模式的细化产生出通过状态机图表规定的 SOV控制逻辑的详细设计 。

表 B. 2 给出了状态转换表的示例 。

表 B. 2 状态转换表

状态/下一状态	转换条件	动作
请求状态		
远程状态	！ 12HS1234D	
远程状态		
请求状态	12HS1234D	
现场状态	12HS1234B ∩！ 12HS1234D	
禁用状态	12HS1234A∩！ 12HS1234D∩12ZSL1234	
现场状态		
请求状态	12HS1234D	
远程状态	12HS1234C∩！ 12HS1234D	
禁用状态	12HS1234A∩！ 12HS1234D∩12ZSL1234	
禁用状态		
请求状态	12HS1234D	
远程状态	12HS1234C∩！ 12HS1234D	
现场状态	12HS1234B∩！ 12HS1234D	

表 B. 2 中的状态转换产生了图 B. 11中的状态转换图 。

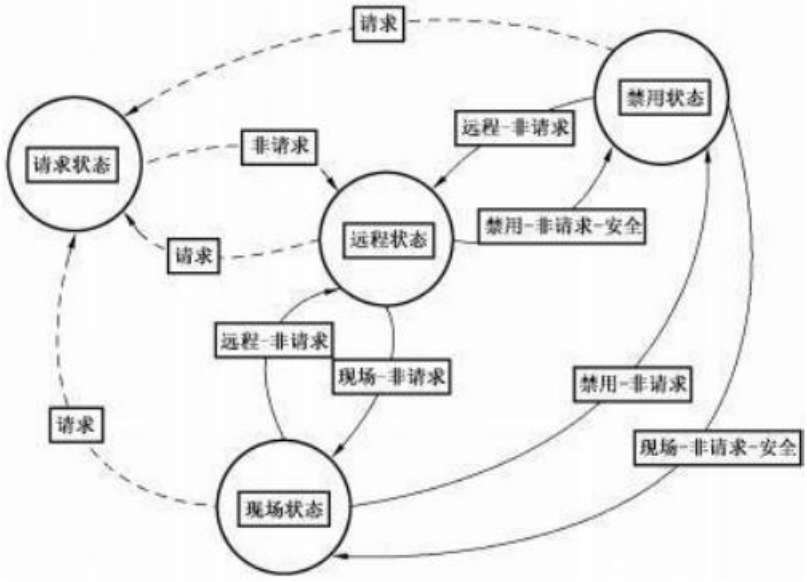


图 B. 11 状态转换图

符合图 B. 6接口要求和图 B. 11的 SOV行为的图形化规范产生了图 B. 12的功能块描述 。

HMI功能和接口无需建模，因为它们仅仅为输出，对 SOV行为没有任何影响 。 因此，图 B. 12可简化为图 B. 13。

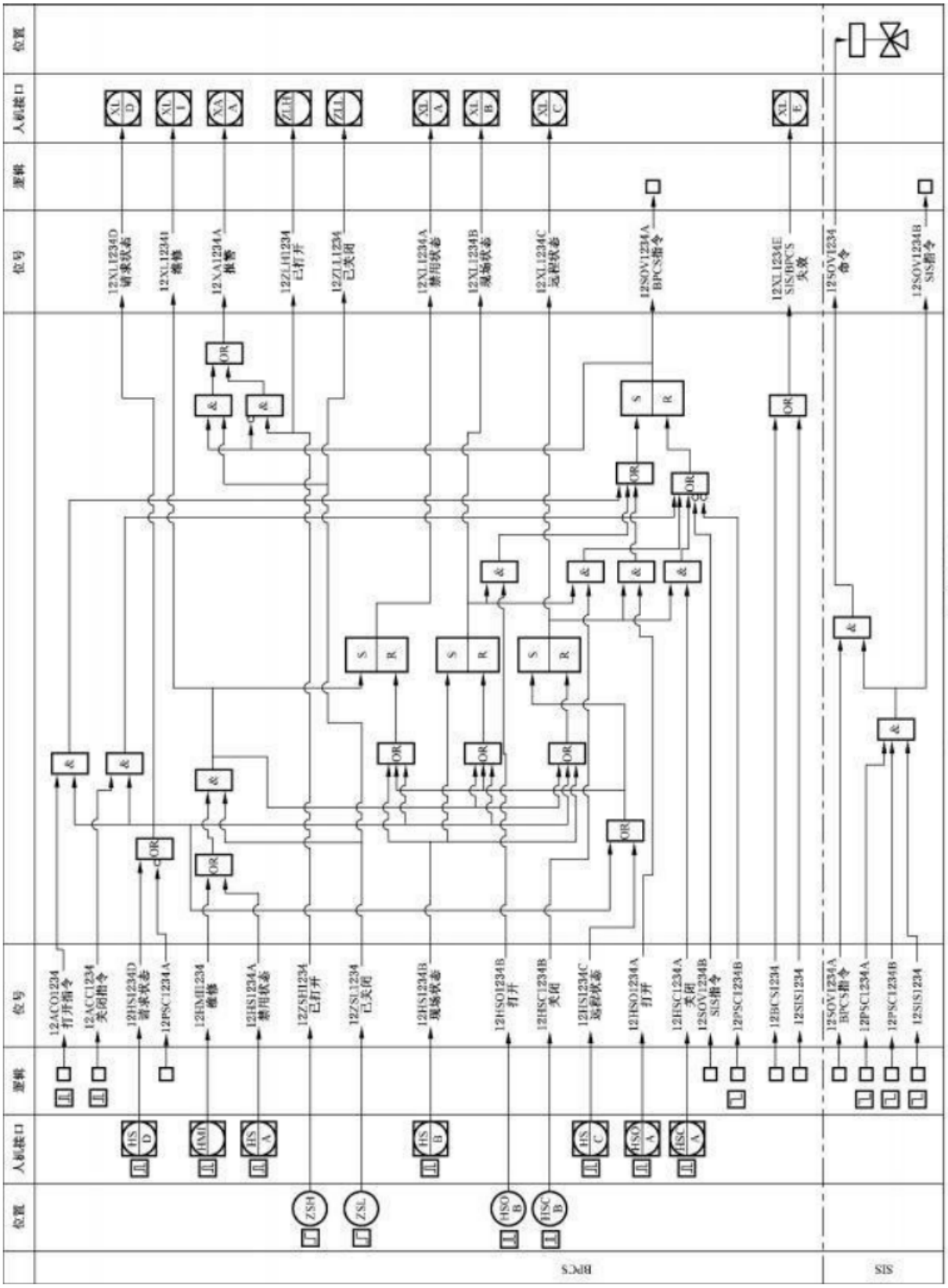


图 B.12 SOV典型逻辑框图

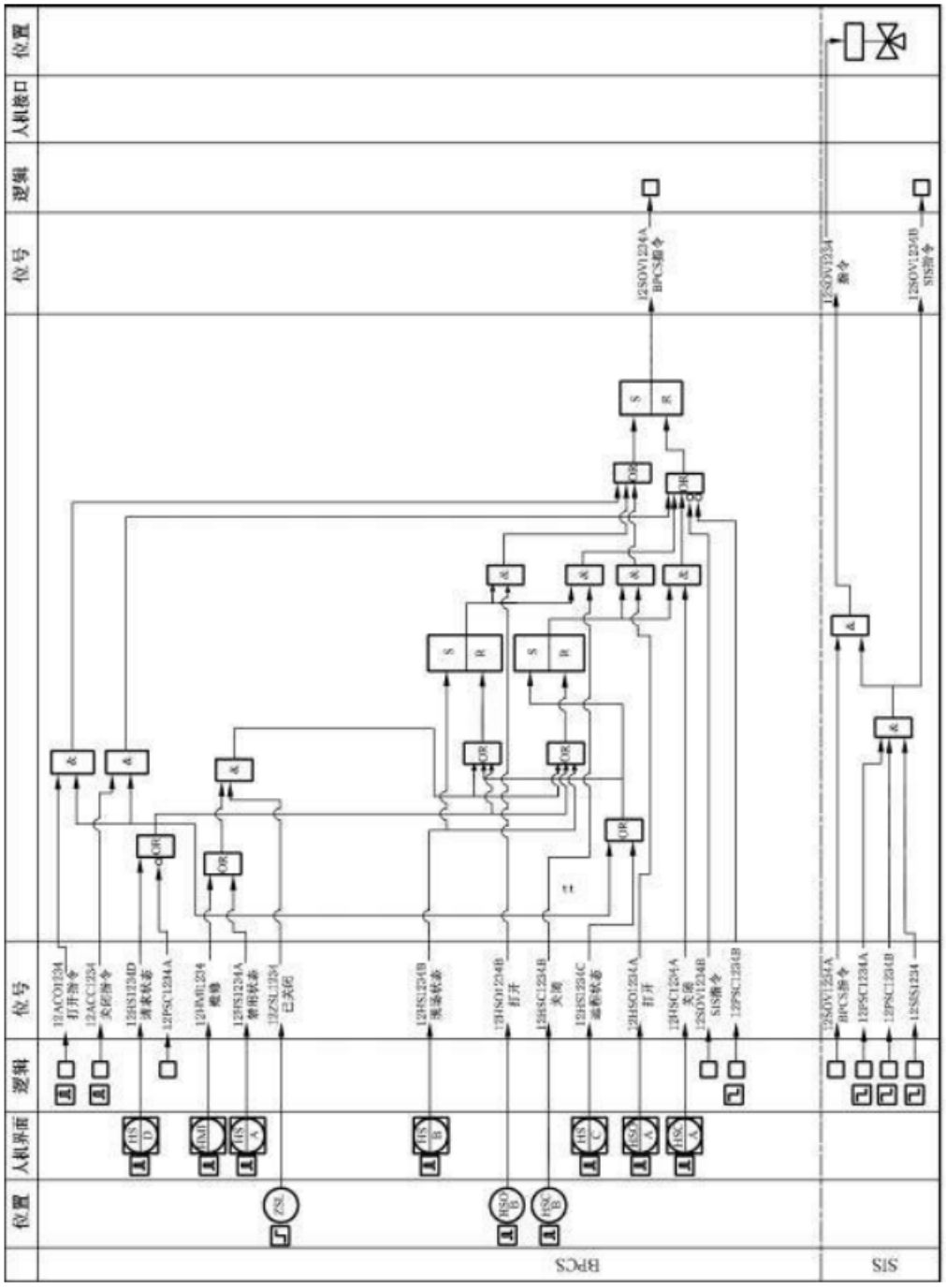


图 B. 13　SOV典型逻辑模块框图

图 B. 13 的规范宜采用模型检查工作台环境的图形化语言来实现 。 这 一 实现考虑了把与 BPCS 有关的逻辑部分以及与 SIS有关的部分分开的需要 。例如 ,这一实现会产生图 B. 14 中关于 BPCS部分的描述内容和图 B. 15 中关于 SIS 部分的描 述 内 容 。 特 别 是 当 BPCS 与 SIS 之 间 存 在 接 口 时 , 为 了 证 明 SIF 与 BPCS 的独立性以及证明安全完整性要求如在任何情况下 BPCS 决不能抑制 SIF 的事实 ,需要对 BPCS部分建模 。 大多数模型检查工作台允许直接实现模型实现 , 而不需要图 B. 12 和图 B. 13 中描述的步骤 ,这些步骤是为了演示的清晰性而提供的 。

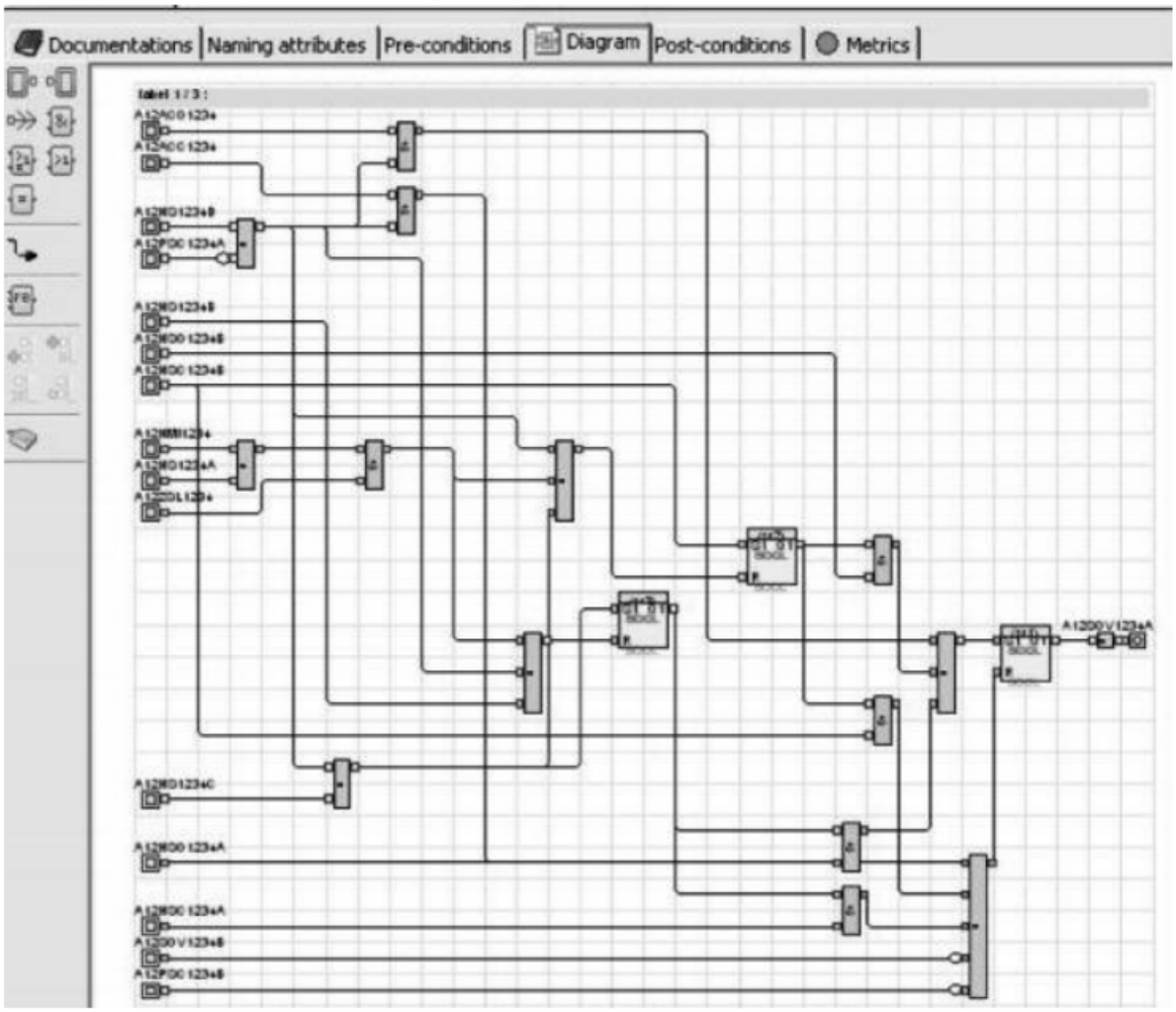


图 B. 14 典型逻辑模块框图实现—BPCS部分

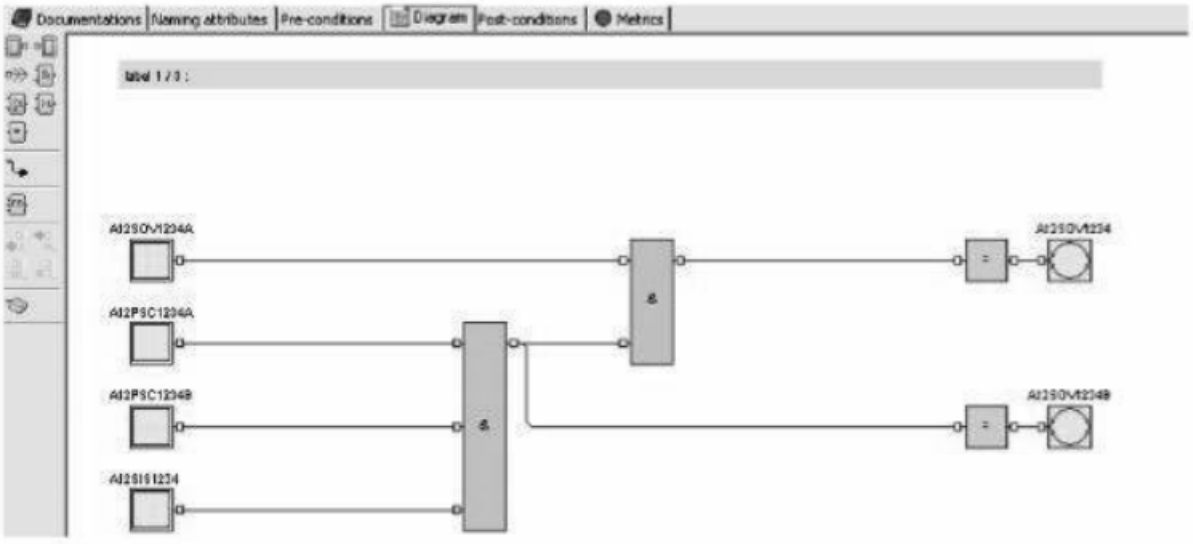


图 B. 15 SOV应用程序典型逻辑模块实现—SIS部分

建模连续性：

建模遵循相同的方法：

—该 SOV 的安全特性；

—将会出现在该示例中的其他必要典型逻辑：

- 2oo3表决；
- 2oo3安全特性；
- 网络通信处理；
- 网络通信安全特性；
- 传感器处理；
- 传感器安全特性 。

B. 4. 3. 4. 2. 2 安全仪表功能层面

在建模的 SIF层面中 ,相同的方法适用：

- SIF02. 01联锁模型；
- SIF02. 01安全特性模型；
- SIF06. 02联锁模型；
- SIF06. 02安全特性模型 。

B. 4. 3. 4. 2. 3 工厂层面

在建模的工厂层面中 ,相同的方法适用：

- 工厂联锁模型：
- 工厂安全特性模型；
- 工厂模型 。

B. 4. 3. 4. 3 模型测试结果和缺陷纠正

为了检测安全行为的违反情况 ,采用模型检查工具独立地运行这些模型 。如果模型检验器发现错误 ,则纠正相关的模型 ,并重新运行 ,直至它们没有这些系统性设计故障 。

B. 4. 3. 5　应用程序集成建模和测试

上述步骤使 AP工程师能够：

— 描述 AP架构;

— 描述功能 AP模块的内容;

—证实架构和模块规范：

- 符合 AP功能规范的要求;
- 符合 AP安全完整性规范的要求 。

在目标物理硬件架构上集成时，这不足以证实 AP概念是切实可行的，因为 AP的功能行为还与物理硬件架构的特性有关 。

该设计阶段包括添加描述AP在目标硬件物理架构中的分布的影响的模型,以便检查仍然满足SRS的要求 。如果情况不是这样,则可能修改 AP模块和/或 AP架构和/或甚至物理架构 。 如果早在AP开发生命周期阶段便已知晓了该物理硬件架构,则可跳过图 B. 10的步骤 。

开发以下模型,并添加到图 B. 16所述的结构的检查模型中 。

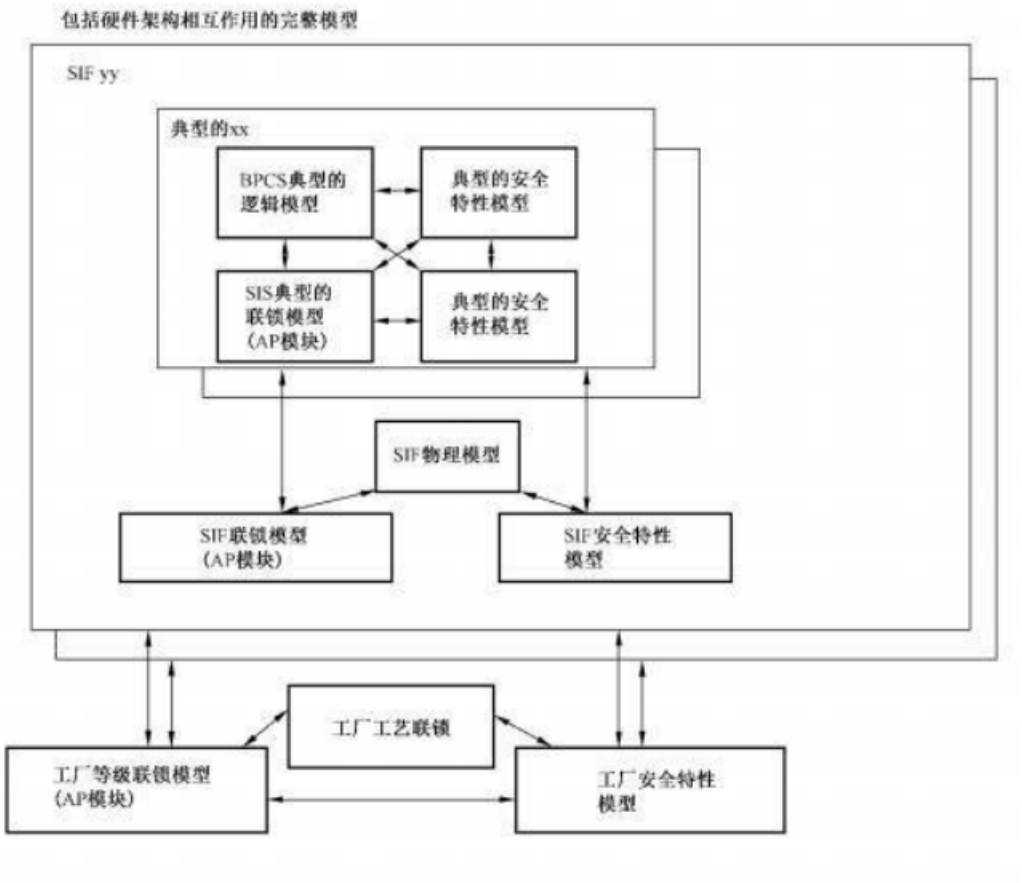


图 B. 16　用于最终实现模型检查的完整模型

B. 4. 4　应用程序的生成

某些AP工作台可以从完成检查过的模型中生成可直接下载的代码。此外,某些工作台则符合IEC 61508的要求 。

B. 4. 5　应用程序验证和测试

当不可能自动从符合IEC 61508或以往使用的工具中生成可下载代码时,需要手动生成和测试 AP。

B. 4. 6　确认

对于采用符合 GB/T 21109. 1— 2022的 12. 6 要求的工具从模型中 自动生成的 AP来说,确认包括通过对模型检查器文件的分析,验证 AP SRS中描述的所有功能和安全完整性特性是否已得到实际证明 。对于一个手动生成的 AP来说,其确认过程在于验证实现严格遵循了模型的假设,并验证实际上已经通过测试证实了 AP SRS中所述的所有功能和安全完整性特性 。

附 录 C
（资料性）
从 NP技术转换为 PE技术时的注意事项

许多过程领域设施在它们的 SIS设计中使用了电气或固态设备 。这些设施可能希望利用 PE技术提供的优势 ,并因此计划通过使用 PE设备对其 SIS进行修改或添加 。在这 一 过渡之前或过渡过程中，可能会为该设施考虑的内容包括:

a) 不宜使用 SIS的 PE设备 ,除非该工厂能成功地验证 、确认 、使用 、操作和维护其 BPCS中的 PE设备;

b) 不宜用 SIS的 PE设备 ,除非该工厂有能力使用 、设计 、修改和维护 PE设备的 AP;

c) 宜执行审核，以确定可从现有工厂应用能力转移到 SISAP的内容 ,包括:

- 技能和经验(例如 ,编程经验 、能力 、可用性)，现场 AP技能对 SIS的可移植性 ,PE支持的管理熟悉程度和参与度;
- 访问安全(本地和远程)能力;
- 模块(例如 ,现有控制算法 ,如电机启动/停止/试运行 、实际位置与位置指令状态的比较)；
- 从硬连线迁移到 PE系统的实时响应和延迟;
- 接 口 (例如，现有接口 、经过证明的接口 、与 DCS的可靠接口 、HMI、网络 、电气接口 、时间特性)；
- 文件(例如 ,能向维护人员/操作人员清楚说明 AP的能力)；
- 为 PE和 AP24/7(一 天 24小时 ,一周 7 天为 24/7)的故障排除提供支持;
- 覆盖范围(支持 24/7的可用性)；
- 响应(例如 ,解决问题的时间)；
- 仿真器(例如 ,用于离线 AP分析 、修改 、开发 、培训)；
- 测试能力(例如 ,针对 AP测试需求的工厂的测试方法和能力)；
- 工厂的旁路规程(以及它们使用应用编程的实现和控制)；
- 从 NP到 PE技术的工厂 HMI方案的转变;
- 培训(可用性 、应用编程的覆盖范围 、HMI)；
- 工具(例如 ,编程 、开发 、测试) ,实用软件的支持;
- 管理支持(现有支持 、充分支持 、各方需求的知晓)；
- 变更程序的管理 ,包括 AP修改的控制 ，以及在已经做出了变更或所做变更可能影响 AP的情况下 ,对安全存储 、配置管理和重新确认规定的控制;
- 系统将来的增强/更新/报废;
- 企业/工厂的应用编程标准以及行业规程的发布;
- 与“姊妹”PE方案在经验互换性 、过程 、设备等方面的兼容性 。

附 录 D
（资料性）
如何从管道与仪表图(P&ID)演变成应用程序的示例

本附录说明了油气分离过程如何从 P&ID图演变成 AP。 图 D. 1 说明了 P&ID。 图 D. 2 利用因果图说明了安全功能的表达 。 图 D. 3用功能块编程显示了因果图到 AP的转变 。

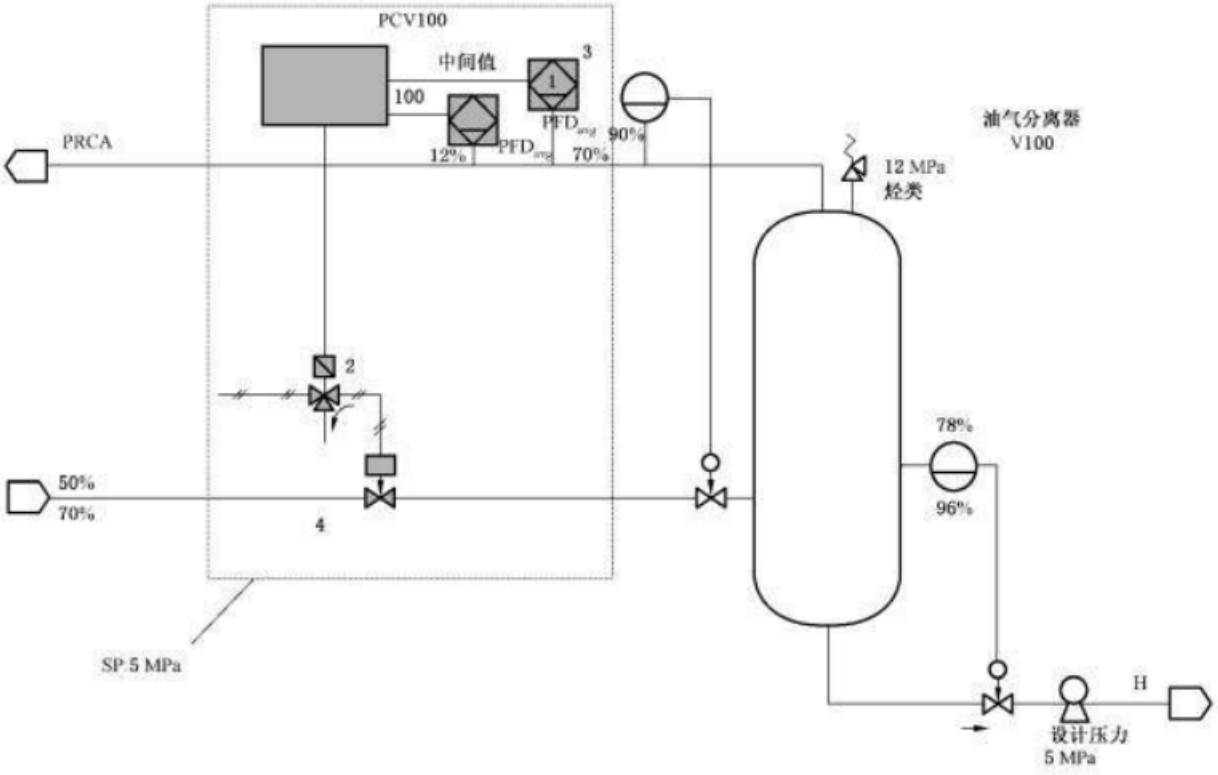


图 D. 1 油气分离器的 P&ID示例

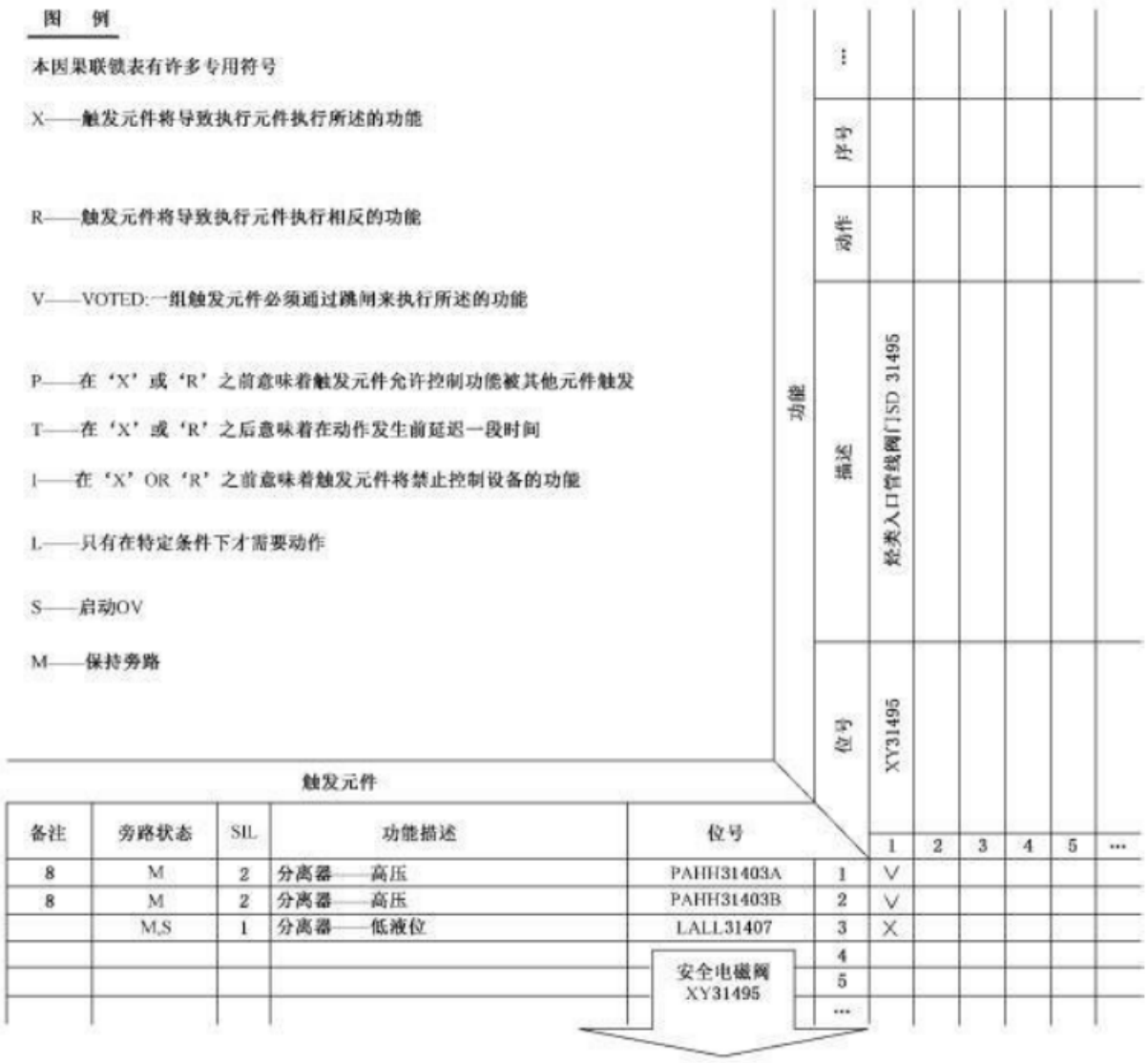


图 D. 2 (一部分)ESD 因果图(C&E)的示例

以下是用于一个 SIF(对压力传感器模拟量信号进行 1oo2表决 ,数字量输出到单个最终元件)的 一个 AP示例 。安全概念是 DTS(失电安全) 。程序语言为功能块 。

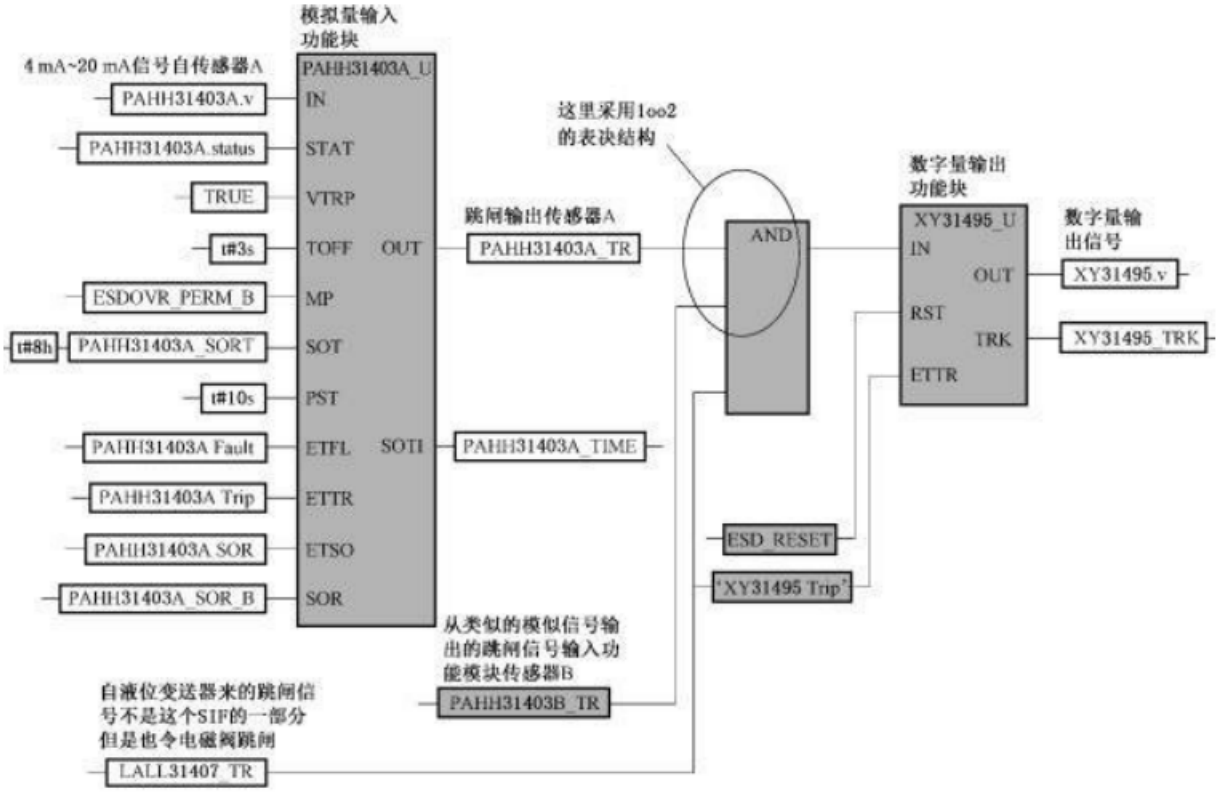


图 D. 3 安全 PLC功能块编程中(一部分)应用程序的示例

附 录 E
（资料性）
用于应用编程的方法和工具

E. 1 用于应用编程的典型工具集

通常，支持 PE编程的工具集将包括以下能力 。

a) 配置编辑器 。这一 编辑器用于配置 I/O SIS子系统 、I/O 内存变量和通信功能 。

b) 语言编辑器 。这些编辑器由应用程序员用于开发执行系统所需全部功能的程序(安全和非安全程序) 。

c) 以往评估过的功能和功能块的库 。这些功能和功能块可在 AP中使用 。

d) 定制的功能和功能块开发能力 。一些供应商提供了 一 个开发环境，允许用户开发可由支持的应用程序语言使用的 自定义功能和功能块 。这些定制的功能和功能块在用于 AP之前，宜进行全面的测试 。

e) AP调度设施 。这些调度设施为设置所需执行顺序及其扫描率提供支持 。

f) 下载能力 。这可以使开发人员将 AP、功能块库 、可变数据以及其他配置信息下载到逻辑解算器硬件中以便执行 。

g) 仿真能力 。有些供应商提供了一个能在支持开发环境的计算机上仿真所有 AP 的开发环境 。这可以在 AP下载到逻辑解算器之前对它们进行完整的离线测试 。

h) 程序监测能力 。这一监测能力可以使用户借助用户定义屏幕或实际功能块或梯形图程序屏幕上的执行程序来查看数据 。这一 开发环境还可提供监测仿真器执行的能力 。此外，可以监测逻辑解算器内执行的程序 。

i) 逻辑解算器的诊断显示 。这些显示表明了系统内主要处理器模块 、通信模块和 I/O模块的状态 。通常显示了每个模块的通过 、失效 、激活状态;在许多情况中，可获得系统内故障的更详细信息 。

PE系统将由支持 AP编码 、应 用 参 数 和 接 口 配 置 以 及 AP执 行 测 试/监 测 的 编 程 环 境 提 供 支 持 。用于安全应用的许多 PE系统将受到专用工具集的支持，配备手册描 述 了 如 何 使 用 这 些 工 具，以 确 保 AP达到预期完整性 。设计环境和应用语言宜具备以下特征 ：

— 控制复杂度的抽象 、模块化和其他特征;AP宜尽可能以经过良好证明的模块为基础，这些模块可包括用户库功能和链接模块的良好定义的规则 。

—对以下内容的表达 ：

- 功能性，在理想情况下，表达为逻辑描述或算法的功能;
- 应用功能中模块化设备之间的信息流;
- 顺序要求;
- 保证 SIF始终在规定的时间限制内运行;
- 避免不明确的行为;
- 保证内部数据项不被错误地重复，所有使用的数据类型已定义，且当数据超范围或坏值时采取合适的动作;
- 设计假设及其相关性 。

— 开发人员以及需了解这一设计的其他人员的理解，包括对应用功能的理解和对技术约束条件的知识 。

— 验证和确认，包括 AP 的覆盖范围 、集成应用的功能覆盖范围 、与 SIS的接口及其特定应用硬

件配置 。

— AP修改 。这些特性包括模块化 、可追溯性和文档化 。

E. 2 应用程序设计的规定和约束条件

为 SIS开发 AP时 ,需考虑 :

a) 将 AP分解为分立的 SIF及其 SIL;

b) 理解每个 SIF的硬件架构 ,在每个 SIFAP中复制这一硬件架构;

c) 如果这会产生复杂程度过高的结果 ,不要优化该 AP(这通常要求由高级程序员来解读 AP) ;

d) 根据供应商的说明(例如安全手册)使用 AP开发技术;

e) 不要将不同 SIF的 AP进行结合;

f) 使用接受过培训 、能够理解和排除故障的 AP语言(例如类型 ,功能) ;

g) 提供与 AP文件中的功能描述一致的 AP书面描述;

h) 根据过程流对 AP进行模块化处理(例如第一个模块为常用 AP,它与 SIF无关 ,但 SIS中却需要它,第二个模块为位于过程入口的第一个SIF,最后一个模块为位于过程出口的最后一个SIF) ;

i) 全面测试(例如模拟 、审查 、审核)每个 AP模块 ,并获得附属的独立的分析(包括此处和所有后续步骤中的操作和维护部门) ;

j) 全面测试构成过程 SIS子系统的模块组合 ,并获得附属的独立的分析;

k) 全面测试 SISAP,并获得附属的独立的分析;

l) 当检查硬件时 ,应用 AP(例如确认与正确传感器/最终元件相关的 I/O) ;

m) 包括过程试运行中 AP的测试(例如不含有害材料的过程运行) ;

示例 :通信链路中的端到端检查 、关于传感器输入的范围检查 、关于数据参数的范围检查以及应用功能的多样化执行 。

n) 在过程转化为设施的过程中(例如试运行) ,AP支持小组成员需在岗;

o) SIF之间无联锁 。

E. 3 用于应用编程的规则和约束条件

以下是一些需要考虑的 PE逻辑解算器应用程序编程规则 ,其有效性取决于应用 。

a) 不使用 SKIP(跳过)和 JUMP(跳跃)功能 。

b) 不使用 NOT(否)功能 。

c) 不使用间接寻址 。

d) 不使用压缩算法 。

e) 不使用基于算术运算结果的逻辑 。

f) 不使用含内部状态存储器的逻辑(例如触发存储器) 。

g) 不在 SIF中使用文本变量 。

h) 不使用包括变量或参数传输的功能或子程序 。

i) 不自定义库功能 。

j) 不使用中断 。

k) 不使用锁存 。

l) 不使用整数变量内部的布尔变量压缩 。

m) 不颠倒逻辑中传感器或执行器的物理状态 。

n) 不将 SIF联锁划分到多个逻辑解算器 。

o) 除被动功能外 ,不使用网络通信功能 。

p) 务必使用工厂认可和经过安全评估的编程方法 。

q) 务必使用标准化模块(例如“典型逻辑”)。

r) 务必提供设备的字母数字描述符,这些描述符给出了与设计图(例如,P&I图、布置图、逻辑图) 一致的每个传感器 、最终元件(例如,电磁阀 、阀门 、电机 、报警装置) 、SIF等的任务描述和交叉引用 。

s) 务必使用工厂批准和之前经过评估的逻辑解算器预编程安全功能(例如 ,急停 、光幕 、安全门) 。

t) 务必将 PE逻辑解算器编程分到输入回路 、逻辑回路 、输出回路这三个单独的区域 :

- 宜将输入回路竖直地画在梯形图格式中,在这 一 格式中,每根横挡的左侧为传感器,右侧设有输入模块 ;每台传感器的接线宜是离散的 ;
- 宜将逻辑图竖直地画在梯形图(或适当的 LVL)格式中 ,在这一格式中 ,每根横挡的左侧为输入值 ,右侧为输出值 ;
- 宜将输出图竖直地画在梯形图格式中 ,在这 一 格式中 ,每根横挡的左侧为逻辑解算器输出值 ,右侧为最终元件 ;每个最终元件的接线是离散的 。

u) 设计方法通常宜为失电即跳闸至安全状态 ;对于需要得电跳闸的系统来说 ,要求采取特殊的防范措施 。

v) 逻辑解算器 I/O寻址和逻辑解算器编程宜安排成反映过程应用的形式(例如 ,初始编程和 I/O分配宜与应用的起始周期有关 ,并在与其过程流命令格式相同的开发过程中继续 ,用停止功能结束) 。

w) 支持功能 ,如检验测试 、手动控制 、旁路 、报警和诊断 ,宜予以识别 ,并与 SIF分开 。

x) 提供必要的备用 I/O、存储和处理能力 ,从而在将来的修改/扩展要求中保持提供必需应用编程的清晰性和能力 。

y) AP(例如 ,输入 、输出 、内部寄存器)对任何部件存在多处使用时,图表宜有指向这些复用位置的交叉参考 。

z) 确保 AP 内的处理顺序满足实时响应的要求 。

附 录 F
（资料性）

通过 SIS项目示例针对使用继电器梯形图语言开发的应用程序的安全生命周期每个阶段进行说明

注 ：本例源于《化工过程安全自动化应用指南》(纽约 1993)，已经获得 ISA andCCPS/AIChE的许可 。本例经改编以符合 IEC 61511的要求 。

F. 1 概述

附录 F 中的示例阐明如何将梯形逻辑应用到安全生命周期实施的每个阶段，以符合 IEC 61511。

这是该示 例 的 第 3 版 。 第 1 版 由 CCPS在 IEC 61508和 IEC 61511之 前 发 布 。 第 2 版 由 ISA (TR 84. 00. 04第 2部分)根据 IEC61508的第 1 版和 IEC61511第 1 版发布 。第 3 版遵循 IEC61508和 IEC 61511的要求 。此外 ,本示例根据 GB/T 21109. 1— 2022图 7安全生命周期的步骤分成几个部分 。

本例的目的是说明一种满足 IEC 61511要求的方法 。读者需要明白 ,IEC 61511以性能为基础 ,有许多方法可用于符合 GB/T 21109。这一示例中运用的一些方法包括 :用于 H&RA的假设分析(what-if)和 HAZOP技术 、用于将安全功能分配给保护层的 LOPA方法 、用于 SIL验证的故障树分析以及记录 AP要求的梯形逻辑 。在 SIS安全生命周期的每个步骤中 ,可以利用这些技术和工具满足标准要求 。

本示例采用了 CCPS/AIChE《化工过程安全自动化应用指南》(1993年)中给出的类似化学过程 。

本示例选择某一过程 的 SIS子 系 统 , 并 应 用 IEC 61511 中 所 讨 论 的 设 计 理 念 、规 程 、技 术 和 验 证 方法 。

本 示例显示了每个 SIF从产生(概念)到生命终结(停用)的各阶段文档 。这一 系列文件给审核人员和工厂人员提供了在 SIS安全生命周期内将 SIF追溯至产生它的过程危险分析(PHA) 的方法 。 每个文 件都清楚地标明了每个 SIF, 以利于生命周期阶段之间的追溯 。 安全的关键组成部分是有能力向他人(例如审核人员 、监管机构 、保险公司)证实每个 SIF提供了足够的风险降低 。

本示例不代表某一 聚合过程的完整设计，因为需要大量细节才能实现高度完整的 、安全的自动化设计 。 因此 ,这一示例包含了许多简化 。

除非另有说明 ,否则出现的所有引用都限于本例中采用的信息 。

F. 2 项目定义

F. 2. 1 概述

本工艺过程是氯乙烯单体(VCM)的聚合过程 ：

$$CH_2 = CHCl$$

为了生产聚氯乙烯(PVC)，

$$[- CH_2 - CHCl-]_n$$

示例中含有危险反应物 VCM ,易燃并产生有毒燃烧产物 ,也是已知的致癌物质 。这 一 工艺过程还说明了较大规模的批量操作 ,此操作以半连续方式在进行聚合作用的 10h左右的时间段内进行 。该示例还简要描述了过程步骤 。

F. 2. 2 概念性计划

一旦决定生产某种产品(本示例中是聚氯乙烯) ,则建立最初的项 目组 。该项 目组首先进行工艺路线的评价，以确定既能满足生产需求 ,又能满足健康 、安全 、安保和环境保护要求的技术 。

F. 2. 3　过程危险分析

在过程评价和项目定义的最初期阶段,过程危险分析小组开始与设计人员紧密互动 。对于项 目涉及的危险物料,该工作组不仅包括工艺设计工程师,还包括健康和安全专家 。该工作组还需经常与其他专家交流,如有相同或类似工艺过程经验的化学家 、操作人员 、顾问或工程承包商,以及工艺包许可方 。在本例中,起始点是基于经过良好实践的工艺过程 。 因此,我们将集中讨论设计过程中影响或直接涉及过程控制系统和安全联锁系统设计的各个方面。 关于设计过程相关方面的更详细信息,可以参阅CCPS/ AIChE的下列文献:

- 《危险评价规程指南》;
- 《化工过程定量风险分析指南》;
- 《高毒性危险材料的安全存储和处理指南》;
- 《气相释放减缓指南》;
- 《化工过程安全技术管理指南》。

F. 3　简化工艺过程描述

用单体生产 PVC相对简单 。该过程的核心是反应器,聚合反应大约需要 10h 的时间完成,在此期间需要机械搅拌反应器内的介质,反应中产生的热量通过反应器夹套的冷却水循环去除 。 由于该过程涉及反应器的批量操作,因此工艺系统设计了多个并联的反应器单元,以便该过程可以在半连续的基础上运行 。为简单起见,这个示例将关注其中一个单元,但需注意实际的生产设施通常有多个并联单元按顺序操作 。

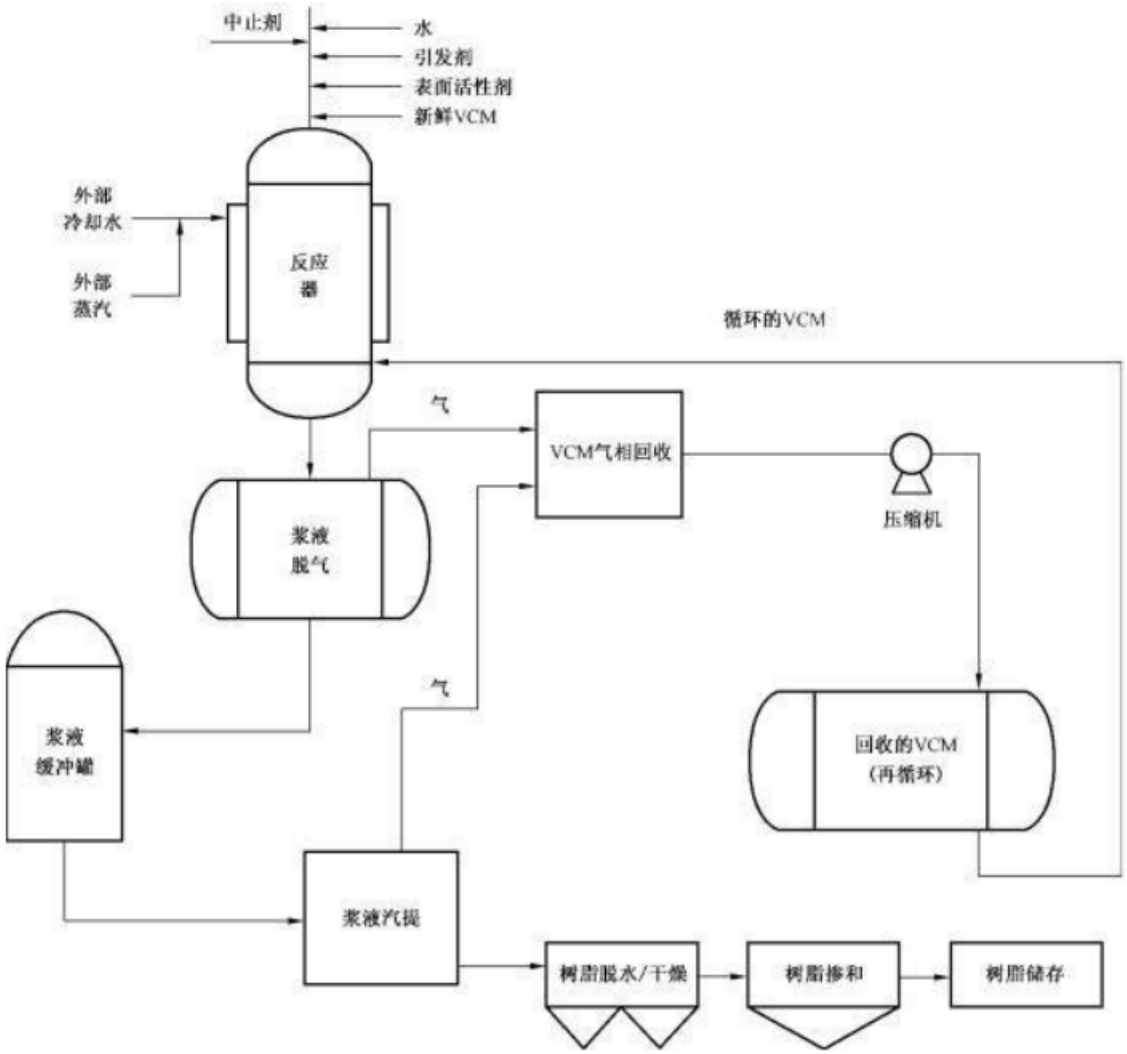


图 F. 1 简化流程图 :PVC工艺过程

图 F. 1是典型 PVC生产设施的简化工艺流程图 。如果在完成最后一批生产并卸料后 ,如果曾打开反应器进行了维修 ,则首先需排空 ,去除气相空间内的所有残余空气(氧气) ,减少单体的氧化反应生成HCl,否则可能导致因应力腐蚀损坏反应器，降低产品质量 。或者 ,先用除垢剂对反应器进行处理，防止在反应器壁上发生聚合 ,然后向容器中注入脱盐水和表面活性剂 。

然后 ,液态氯乙烯单体(VCM)在其相应的蒸气压(21℃时约 0. 386MPa)下加入 。

该反应的引发剂为溶于溶剂的过氧化物 。 由于它相当活跃，因此需将它储存在低温的专用仓库 。在生产过程中会取出少量用于日常使用 ,并保存在冷冻箱中 。先将引发剂注入到 一 个与反应器相关联的小型装料罐中，以保证只加入正确的量 。

注入反应的引发剂后 ,用蒸汽将水加热并加入到反应器护套中，以便将温度升高至 54. 5 ℃~60 ℃(由特定产品的批次配方决定) ,这样才会以合适的速率持续进行反应 。为了使 VCM悬浮在脱盐水中，则需要搅拌(控制颗粒尺寸) ,提高整个批量中的热传导 ,并生成均匀的产物 。 由于是放热反应 ,冷却水在容器夹套内循环，以控制反应器温度 。在完成聚合所需的大约 8 h 内 ,严格控制反应器条件 。

当反应器中的压力下降时 ,反应完成，表明大部分单体已经反应 。 反应后的聚合物从反应器中卸出 ,送到下游工艺单元进行残留的 VCM 回收 、汽提 、脱水和干燥 。

F. 4　初步设计

审查所有当地的特别要求,确定适用的法规,并建立一般风险指南 。对公用设施要求(如气源 、冷却水 、电力)进行审查,确认满足应用要求 。

F. 5　IEC61511 应用

F. 5. 1　概述

当初步规划完成后[见 F. 2~F. 4(含)],开始实施 IEC 61511。

对于本例,设计策略是初始化生命周期设计(图 F. 2),并将生命周期阶段分解为 10个步骤,与图F. 2和表 F. 1(安全生命周期概述)保持 一 致 。在该节点上,使用生命周期表来分配每个生命周期阶段的职责可能是有益的,如表 F. 1所示 。

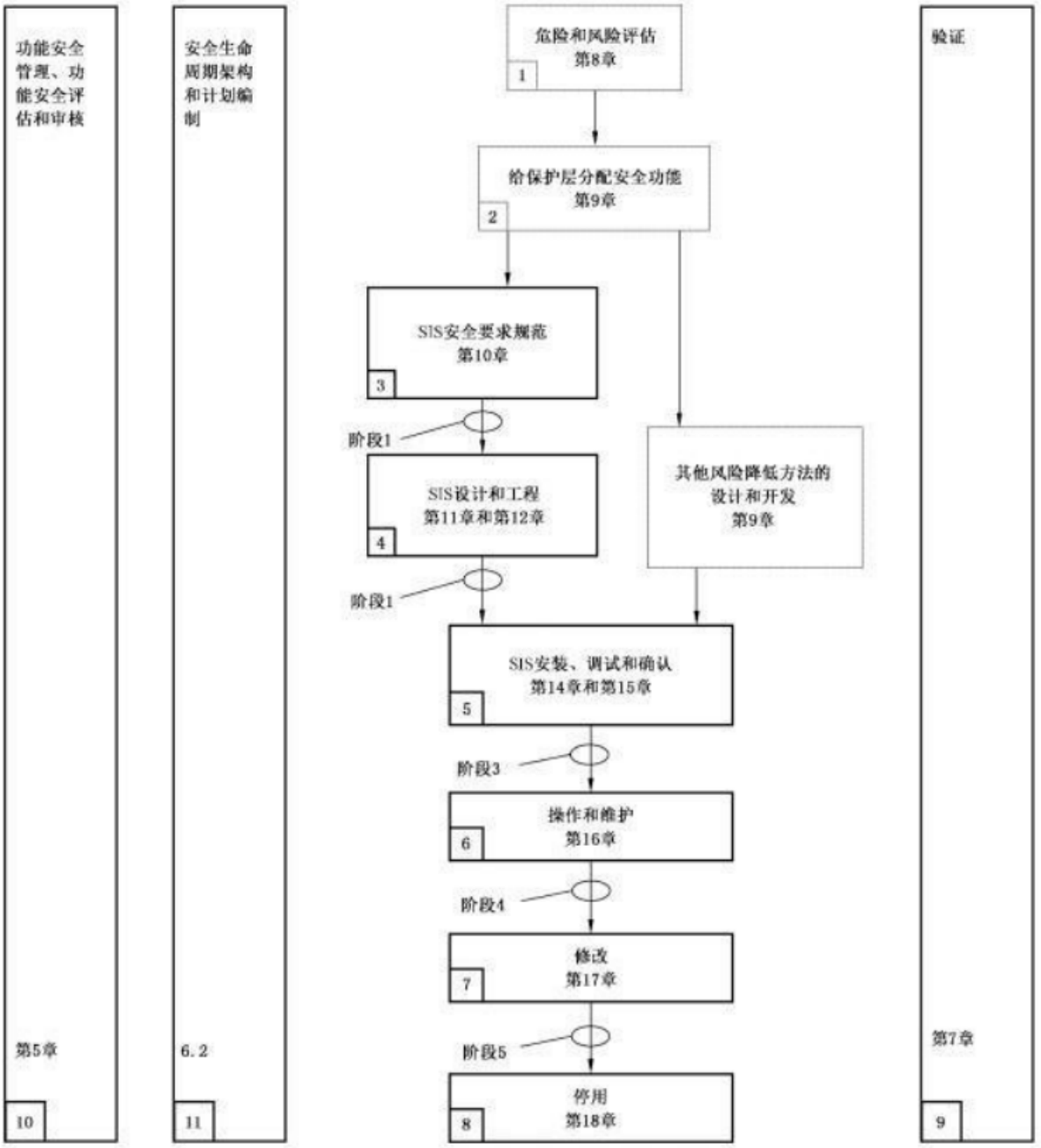


图 F. 2 SIS安全生命周期阶段和 FSA 阶段

表 F. 1 SIS安全生命周期概述

安全生命周期阶段或活动		目标	GB/T 21109. 1—2022 的要求章节或小节	输入	输出	责任方
图 F.2方框号#	标题					
1	H& RA	确定过程及相关设备的危险和危险事件、导致危险事件的事件顺序、与危险事件相关的过程风险、风险降低要求和达到必要的风险降低所需的安全功能	8	过程设计、总图布置、人员配备、安全目标	危险、所要求安全功能和相关风险降低的描述	PHA小组见F. 2. 2
2	将安全功能分配给保护层	将安全功能分配到保护层，并为每个SIF分配相应的 SIL		要求的 SIF和相关安全完整性要求的描述	安全要求分配的描述（见GB/T 21109. 1—2022 的第 9章）	PHA小组见F. 2. 2
3	SISSRS	为了达到要求的功能安全，根据要求的SIF及其相应的安全完整性规定每个SIS的要求	10	安全要求的分配描述（见GB/T 2109.1—2022第 9章）	SIS 安全要求； AP 安全要求	电仪小组
4	SIS设计和工程实施	设计 SIS 以满足 SIF及其相应的安全完整性要求	11 和 12. 4	SIS安全要求； AP安全要求	符合 SIS 安全要求的SIS设计； 制定 SIS 集成测试计划	电仪小组
5	SIS 安装、调试和确认	集成和测试 SIS 根据要求的 SIF及其相应的安全完整性，确认 SIS在各方面都满足安全要求	12.3、14、15	SIS设计； SIS集成测试计划； SIS安全要求； SIS 的安全确认计划	SIS 的全部功能符合设计； SIS 集成测试的结果； 安装、调试和确认活动的结果	建造方
6	SIS 操作和维护	确保在操作和维护期间保持 SIS 的功能安全	16	SIS安全要求； SIS设计； SIS 的操作和维护计划	操作和维护活动的结果	运行方

表 F. 1 SIS安全生命周期概述 (续)

安全生命周期阶段或活动		目标	GB/T 21109. 1—2022的要求章节或小节	输入	输出	责任方
图 F.2方框号 #	标题					
7	SIS变更	对SIS进行校正、增强或改造以确保达到和保持要求的 SIL	17	修改后的SIS安全要求	SIS修改结果	运行方
8	停用	确保适当的审查,获得授权,并确保SIF适当保留	18	竣工安全要求和过程信息	停用的 SIF	运行方
9	SIS验证	测试和评估给定阶段的输出,以确保作为该阶段输入的产出和标准的正确性和一致性	7. 12. 5	每个阶段SIS的验证计划	每个阶段SIS验证的结果	运行方
10	SISFSA	对SIS所达到的功能安全进行调查并做出判断	5	SISFSA计划编制 SIS安全要求	SISFSA结果	运行方

F. 5. 2 第 F. 1 步 :危险和风险评估

生命周期阶段见表 F. 2。

表 F. 2 SIS安全生命周期— 方框 1

概述					
安全生命周期阶段或活动		目标	GB/T 21109. 1—2022的要求章节或小节	输入	输出
GB/T 21109. 1— 2022的图 7,方框 1	H& RA	确定过程及相关设备的危险和危险事件、导致危险事件的事件顺序、与危险事件相关的过程风险、风险降低要求和达到必要的风险降低所需的安全功能	8	过程设计、总图布置、人员配备、安全目标	危险、所要求安全功能和相关风险降低的描述

F. 5. 3　危险识别

危险识别过程始于业务决策分析期间(F. 2) 。这是 PHA 小组最重要的职能之一,并 一 直持续到该过程移交给工厂运行方并接受运行安全审查和审核程序为止 。

F. 5. 4　初步危险评价

工艺过程开发计划的第一 步是识别生产过程的所有参数 ,确定安全和环境危险(或危险事件) ,尽量使过程实现固有安全 。为了实现这一点 ,需要提供潜在替代工艺过程中涉及到的所有进料 、中间物 、产品和废弃物的物理和危险特性 。例如 ,使用单体生产特定的聚合物产品时 ,基本反应物几乎无其他选择 。可替换的工艺过程是聚合中间产物 、悬浮物或乳剂 。表 F. 3 中概括了 VCM 的重要特性(在 “实际的　例子中需要使用最新的 VCM化学品安全技术说明书) 。

然而 ,为了保证能安全地控制反应率 , 防止出现失控反应 ,在满足产品质量和产量的同时 ,需要仔细选择反应条件和引发剂(以及添加剂) 。选定的技术涉及水中聚合 ,但确实需要少量相对危险的液态引发剂 。此外 ,还需密切关注与引发剂相关的危险 ,但这些危险均不包括在本简化示例中 。

F. 5. 5　事故历史

接下来 ,对危险进行识别 。在本例中 ,主要的危险与来源于 VCM 的易燃性和燃烧产物的毒性 。在实际的装置设计中 ,人员暴露率和环境中 VCM 的限值也是主要的考虑因素 ; 为了简单起见 ,这些考量均不包含在本例中 。作为第一 步 , 回顾以往类似操作相关的事故历史是非常有用的 。

在 VCM 的实例中 ,某 PVC装置发生事故 ,4人死亡 ,10人受伤 。这次事故是由于从错误的反应器中卸出一批次单体 ,导致单体泄放到并联反应器所在厂房内 。　VCM 蒸气可能被电机的火花或静电点燃 ,反应器所在的厂房发生爆炸 。

在另一起事故中 ,工人错误地打开了处于操作中的反应器上的人孔盖 , 释放出大量氯乙烯 , 引燃后造成闪火 ,导致一名维护人员和两名工人死亡 。

还有一次事故是在反应器底部阀门打开的情况下向反应器充注了 946 L VCM 。　虽然这次释放造成了严重危险 ,但并未引起燃烧 , 因此没有人受伤 。还记录了其他几次事件 ,如在氯乙烯泵维护过程中 , 发生了爆炸(三个同时发生的异常情况产生过氧化物污染物) 。在定期充填的过程中 , 由于柱塞阀的维护问题 ,VCM也曾从 VCM生产装置的洗涤器中泄漏出来 。VCM 的燃烧造成了一人死亡和多人受伤 。

还有一些与运输有关的 VCM泄漏和火灾 。　在美国得克萨斯州休斯顿附近发生的 16 节槽罐车脱轨的事故中 ,VCM从 182 000 L 的槽罐车中泄漏出来 后 立 即 燃 烧 。　在 火 灾 中 暴 露 45 min后 , 另 一 节 VCM槽罐车破裂 ,产生一个巨大的火球 , 导致 一 名消防员丧生 , 另有 37 人受伤 。爆炸后 ,槽罐车的大部分在距离脱轨现场大约 120 m外的位置被找到 。

此外 ,对于所报告的每次重大事故 ,可能有大量的小事件 。要关注可能发生的小泄漏 , 因为这些可能会成为重大事故的导火索 。特别是对于高度易燃的承压物料 ,小泄漏量的点燃如果使其他系统设备受热 ,可能会导致更大的失效 。　因此 ,VCM 系统的完整性需有较高等级 。

表 F.3 氯乙烯的一些物理特性

分子式 :CH_2 = CHCl 名称:氯乙烯单体(VCM) 单氯乙烯 氯乙烯(VCl) 作为压缩液化气体运输;饱和蒸汽压力(RVP) = 0.517 MPa 气体,无色,气味芳香;摩尔重量 =62.5;相对密度(蒸气) = 2.16 正常沸点 = - 13.4 ℃ ;相对密度(液态正常沸点) =0.97;浮在水上,并在水上沸腾 临界温度 = 157.85 ℃ ;临界压力 = 5.54 MPa;熔点 = - 154 ℃ 汽化热 = 372.16 kJ/kg;燃烧热 = 18 924kJ/kg 聚合热 = 1 695.6 kJ/kg;在环境条件下通常是稳定的;暴露在空气、光照、潮湿、热或自由基引发剂的情况下会聚合,除非通过抑制剂稳定
火灾危险 : 空气中的燃烧极限 :3.6% ~ 33% 闪点 : - 61 ℃(开杯闪点) ; 自燃温度 :472 ℃ 喷射、沸腾并产生比空气重的气体云,该气体云可能会被回火点 。 着火后会产生有毒气体(HCl、CO等) 。 如果在有限空间被点燃,则可能会爆炸 。 如果容器暴露在外部火灾中,可能会导致 BLEVE
健康危险 : 蒸汽会刺激眼睛、鼻子和喉咙 。 如果吸入,则会导致头晕、呼吸困难,并可能会造成严重的负面影响甚至死亡 。 过度暴露可能会对肺部和肝肾造成影响 。被 OSHA、国际肿瘤研究机构(IARC) 和美国国家卫生研究院国家毒理学计划(NTP)列为人类致癌物质 。 阈值 :5 mg/L OSHA安全限值(PEL) :1 mg/LTWA,在不超过 15 min的任何时段内,平均偏移限值为 5 mg/L。 嗅觉阈值 :260 mg/L 接触液体可能会导致冻伤
水污染 : 工艺用水中的限值 :10 mg/L 场外排放水的限值 :1 mg/L
空气排放 : 大气排放过程中的限值 :10 mg/L(当地标准) 厂界年浓度限值:空气中为 0.2 μg/m^3 VCM
泄漏响应 : 发出警报— 高可燃性,消除点火源,通风 停止流动 疏散该区域,只有佩戴适当防护装备的人员才可进入 。 大火时任其燃烧;小火时用干粉或 CO_2 扑灭 。 用水冷却暴露的容器 。 防止进入污水管道系统,避免潜在的爆炸

F. 6　初步工艺过程设计的安全考虑

在此例中，PVC的预期产量为 9 万吨/年，或约为 10400kg/h。基于已知的反应动力学，在 60 ℃左右的反应温度中，相应的循环时间大约为 8 h。反应器容量的选择需基于对以下事实的了解：与危险介质总量相关的灾难性容器失效的危险量级。 一种极端情况下，仅使用单台反应器，每一批次是在40%的浆液混合物中生产 81. 6 tPVC，反应器容量需要 189000L。这可能是不明智的，因为没有冗余，而且有非常大的易燃、高压物料存量。 同样，由于生产能力未分散开，每批产量将会很大，频次低，因此对下游设备的存储容量要求较高。此外，需要向反应器添加大量危险的引发剂，这足以引发严重的安全问题。

另一种极端情况是使用多个小型反应器(例如，十台)，每台一个批次的产量为 8. 16 t，大约 18900L。第一种极端情况的储存量非常大;第二种极端情况的产量较小，切换操作会更频繁，有更多的互连管道、阀门，复杂程度也会更高。根据操作需求、设备可用性、成本和安全性，考虑最优方案。

基于以上分析，选择并联反应器的数量和反应器单元的大小。 这将为未来的产能扩张提供潜力。在此例中，决定安装三台并联的反应器，每台反应器有 64400L 的生产能力。 每一批次所要求的 20L 引发剂在安全处理的可控数量内。反应器中 VCM 的最大存量预计为 27. 2 t。

选择反应温度的目的是达到想要的分子量，这是由最终用途决定的。为了实现反应器的稳定运行，需要适当控制反应器的冷却水温度，以防止出现失控反应。 聚合反应温度的稳定控制要求冷却水与反应温度之间的温差非常小。对于这此例来说，为了实现安全运行，对于 60℃的反应温度，冷却水的温度要足够高，从而使温差非常小。冷却水的供应足够可靠并有足够的量且压力合适。

在此例中，假设安全阀和泄放阀排放至洗涤器，不会造成环境事件。

F. 7　识别出的过程危险

与 VCM泄漏有关的主要重大危险是火灾和爆炸，并产生毒性燃烧产物。这些类型的危险包括：

a) 喷射火：来自压力系统的泄漏会被点燃，并形成喷射火，可能会对其他设备造成影响和损坏。(据粗略估计，喷射火长度大约为喷射口直径的 150倍，即从 50mm孔洞喷射出的火焰长度可能会达到大约 9 m)

b) 闪火：带压液体泄漏会导致闪火，产生的易燃性蒸气移动至点火源。点燃后，火焰通过易燃性蒸气云向后移动。 (在这种情况下，可燃性烟羽可能会明显大于喷射火焰)

c) 池火：来自瞬时泄漏的残余液体形成积洼，它可能会燃烧，燃烧时的火焰高度是积洼宽度的两倍到三倍。

d) BLEVE(沸腾液体扩散蒸汽爆炸)：如果 VCM 的压力储罐或相连的管道暴露在外部火灾中，可能会失效。这一失效可能会造成灾难性的压力储罐失效、火球和抛射碎片。 泄压阀的超压保护无法预防 BLEVE。

e) 爆炸：易燃气体泄漏到有限空间内，如果被点燃，则可能会引爆或严重超压爆炸。

f) 液压失效：储罐过量充装后，液体通过加热膨胀破坏气相空间将快速增压，继而可能会产生储罐突发失效。

g) 应力腐蚀失效：系统中的空气(氧气)可能会使氯离子增多，并可能会导致金属完整性的丧失。

h) 有毒燃烧产物：VCM 的燃烧产物包括光气、氯化氢、一氧化碳以及其他有毒物质。 (这些产物会在火灾过后出现，特别是如果火灾发生在有限空间内)

i) 聚合反应失控：VCM 聚合反应失控可能会导致反应器破裂，将产生大规模的 VCM 泄漏。

此外，VCM具有慢性接触危害，是致癌物质，它是一种管控物质，当人暴露于 VCM气体中时，在空气中暴露时间超过 8 h 的 OSHA PEL(人员暴露极限—时间加权平均值) 为 1 mg/L(暴露时间为 15 min时限值为 5 mg/L)。另外，一些国家和地区条例限制它从工艺通风口和工厂水处理系统中排放。

关于可能出现在 PVC产物中残余 VCM 的量，也有严格的限值规定 。

还有一些较小的短期危害，包括可能吸入 VCM气体以及被闪蒸液冻伤 。人们需要加以防护，避免受到吸入和潜在冻伤的影响 。

在这一节点，对危险区域的范围进行预估，来显示重大潜在事故的程度大小 。 释放 27. 2 t的 VCM可能会产生等效于边长为 120m 的立方体的易燃蒸气云 。 由于 VCM气体比较重，可能含有气溶胶，大规模的蒸气云更有可能成为圆盘状，但易燃物面积直径仍然可能达到 300m~450m。这表明，单台反应器的最大事故可能影响到装置区以外，并可能会使有限空间充满易燃气体 。根据下表 F. 8 中所述的评估准则，需将这一影响至少考虑为“严重”，但也有可能是“大范围的”，取决于具体的数据 。保守起见，PHA小组将其划分在“大范围的”影响类别中考虑 。

注 ：大量储存在现场区域的 VCM未纳入此例考虑 。

F. 8 工艺过程设计定义策略

设计细节要求确定该设施的基本操作规程和维护策略 。 为了有助于这项工作的顺利进行，给出图 F. 3,初步 P&I图 。该工艺过程的操作步骤概述如下：

a) 预排气 :如果反应器因维护被打开过，鉴于质量和完整性的原因，需要将氧气从系统内排空 。

b) 反应器准备:用高压水冲洗空的反应器,如果打开了人孔,则需进行泄漏测试,并用除垢剂处理。

c) 脱盐水充装 :加入预定的水量 。过度充装将会导致出现液体溢流;充装过少可能会导致质量问题和潜在失控反应 。在这一 步骤中，还引入表面活性剂或其他添加剂 。

d) VCM充装 :将准确数量的 VCM加入到反应器中 。

e) 反应器加热 :将引发剂从充装罐加入至批料中，将蒸汽加入至反应器冷却水夹套循环系统中，直至批料达到反应温度(大约比稳态反应温度低 5. 5 ℃) 。

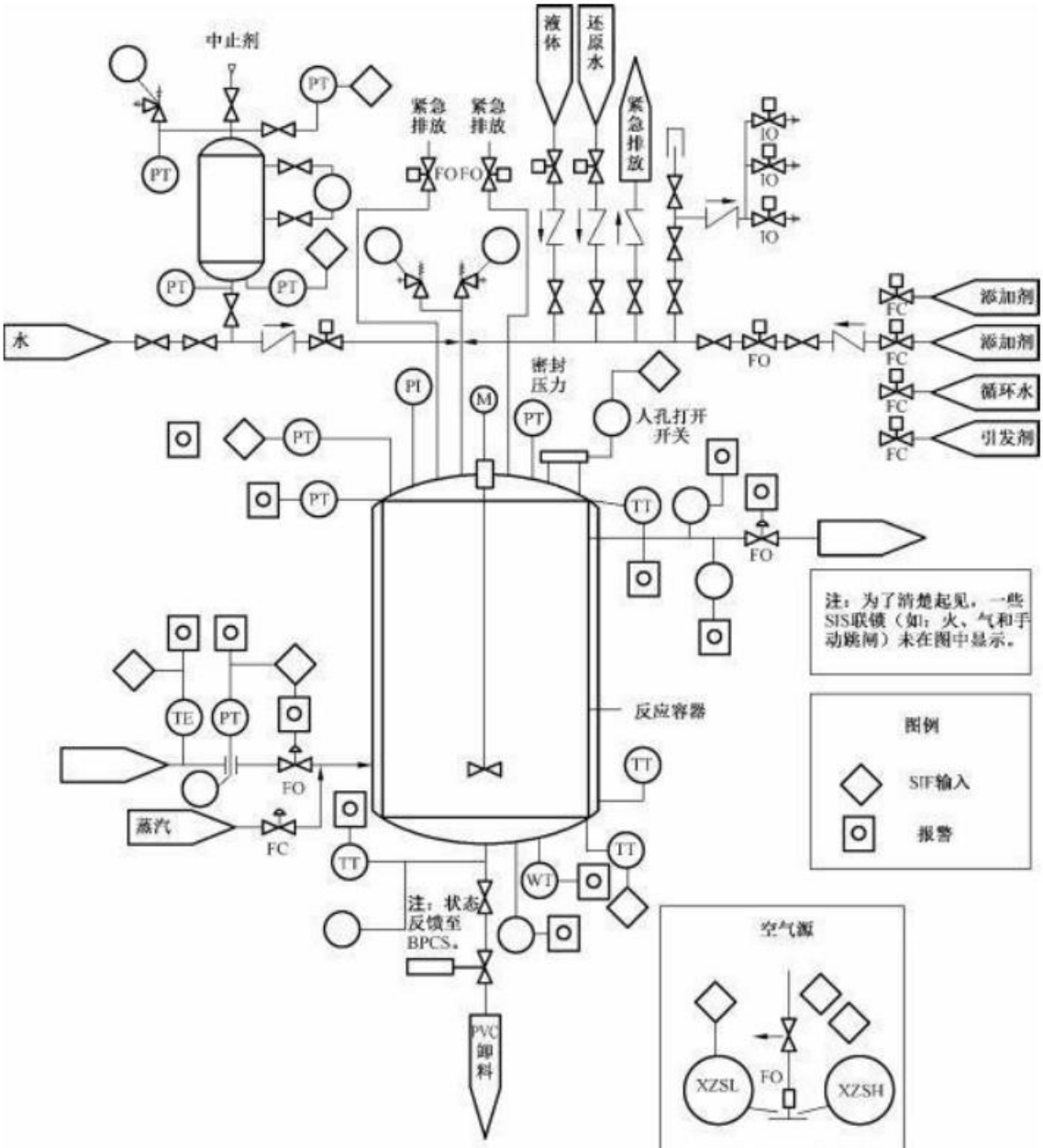
f) 反应 :切断蒸汽系统，改为冷却水通过反应器夹套循环，在进行反应时，通过撤除聚合反应的热量来控制温度 。

g) 终止：当由于所存在的大多数 VCM 被聚合反应消耗完，反应器的温度开始下降时，该批次将进行卸料 。

h) 反应器卸料 :借助压力将反应器物料排卸至下游的设备中，进行脱气处理，以便用于后续的汽提和干燥过程 。为了防止树脂在反应器中沉积，搅拌器在卸料过程中持续运行 。 回收未反应的 VCM，以便重新使用 。

为紧急情况提供了两套额外的工艺系统 。在出现不受控反应或可能发生此类事件的情况下，可向该批料加入中止剂，从而快速停止聚合反应 。需要对批料进行搅拌，以便很好地分散中止剂，快速停止聚合反应 。如果搅拌器失效，则需在一两分钟内加入中止剂，可以在反应器内的液体旋涡消失之前完成混合 。作为备选方案，反应器物料可通过“鼓泡”来混合— 降低压力，以便在整个液体浆料中产生上升的气泡 。 以上都由操作人员人工触发 。

第二个紧急系统为自动泄压系统 。 出现失控反应时，可通过将反应器压力泄放至排放系统来保证安全 。将沸腾反应物质的气化热安全地从反应器中移除 。需确定该紧急排放系统的能力，确保能处理反应器系统的峰值排放需求 。



项目#	修订版次 #	修订	修订人	审核人	批准人	日期

项 目 # YYYY　　日期；
制图人 :S. Bulk
审核人 :V. May
R. Brown
批准人 :W. Burk
图纸号 ：# XXXXX1

图 F. 3　用于 PVC反应器单元的初步 P&ID示例

为了清晰起见，图中简化标示管道连接处细节 。详细图示见图 F. 11。

F. 9 初步危险评估

F. 9. 1 概述

当设计达到某种详细程度时，PHA小组对设计开展初步的危险评估 。 因为设计还不完整，此评估是初步评估 。 PHA 小组将假设分析(what-if)/检查表审核(表 F. 4)用于该过程较简单的部分，将HAZOP(表 F. 5)用于该工艺过程较复杂的部分 。

根据危险识别过程和以往的事故历史，该示例中的过程反应器涉及从“轻微的”到“大范围的”事件可能性，如表 F. 8 中定义的 。

此外，设计完整性需考虑严密性要求，以防止出现可能会危害人身安全和健康的 VCM 泄漏事件 。需将危险审核的结果完整地记录下来，特别是可能导致不受控泄漏的事件顺序 。

表F. 4和F. 5仅列出了与此例相关的部分危险清单。 在典型项目中，将会有更全面的假设分析(what-if)和 HAZOP分析项清单 。表 F. 4 和表 F. 5 由过程危险分析小组编制和审批，见 F. 2。

表 F. 4 假设分析/检查表

假设分析 …	危险	后果	保护措施	参考 #	建议	执行人
如果大面积停电该怎么办?(UPS仪表电源仍正常供电)	由于失去搅拌而出现失控反应。 通过搅拌器电机停止、冷却液流量低、反应器压力高和反应器温度高来体现	失控反应会导致反应器过压，以及密封失效	加入中止剂，并使反应器“鼓泡”，来停止失控反应。 反应器-SIS泄压（为这一事件确定压力安全阀的大小）		使用 LOPA 确定所要求的 SIL	
批料配方错误—使用了两倍充装量的引发剂	高浓度的引发剂会导致失控反应。 通过反应器的高温和高压来体现	失控反应会导致反应器过压，以及密封失效	加入中止剂 。 反应器-SIS 泄压(为这一事件确定压力安全阀的大小)		使用 LOPA 确定所要求的 SIL	
如果反应器搅拌器的密封失效该怎么办	VCM烟气泄漏。通过反应器密封内的高压以及这一区域内的烟气探测器来显示	VCM 烟气是易燃物	在反应器密封四周加强额外通风 。 通过高密封压力-SIS 来实现反应器减压		使用 LOPA 确定所要求的 SIL	
注 ：这里仅列出一部分危险 。						

表 F. 5 HAZOP

引导词(GW)	偏差	原因	后果	保护措施	参考	建议	执行人
无	无流量	冷却水控制系统失效	最终会造成失控反应,通过反应器高温和/或高压体现	加入中止剂量。 反应器-SIS泄压(为这一事件确定压力安全阀的大小)		使用 LOPA 确定所要求的 SIL	
		由于泵断电导致泵停止运行	最终会造成失控反应,通过反应器高温和/或高压体现	除了电源外,泵还有蒸汽驱动。 加入中止剂。 反应器-SIS泄压(为这一事件确定压力安全阀的大小)		使用 LOPA 确定所要求的 SIL	
无	无搅拌	搅拌器电机驱动失效	降低冷却效果,温度不均匀,导致失控反应。 通过反应器高温、高压和搅拌器电机电流低来体现	加入中止剂,并使反应器“鼓泡”,以便停止失控反应。 反应器-SIS泄压(为这一事件确定压力安全阀的大小)		使用 LOPA 确定所要求的 SIL	
更多	温度较高	温度控制失效导致在蒸汽加热过程中过热	高温导致失控反应。 通过反应器高压和高温来体现	加入中止剂。 反应器-SIS泄压(为这一事件确定压力安全阀的大小)		使用 LOPA 确定所要求的 SIL	
更多	液位较高	液位控制失效导致反应器过量充装	温度上升,反应器充满液体,可能会导致反应器出现液压损坏和 VCM泄漏。 通过充装液位高、充装重量大或反应器压力高来体现	将液位和重量与配方比较。 反应器-SIS泄压(为这一事件确定压力安全阀的大小)		使用 LOPA 确定所要求的 SIL	
注:这里仅列出一部分危险。							

根据这些结果,由适当的工艺过程和仪表专家组成的 PHA小组汇总了一份意外事故事件清单,其中,指定 SIF作为危险的减缓措施。

表 F. 6 为意外事故事件以及相关预防策略的部分清单,也是用于提出联锁策略和动作以便进一步识别或设置附加独立保护层的相关预防策略。表 F. 6 由过程危险分析小组编制和审批,见 F. 2。

表 F. 6　用于制定 SIF策略的部分危险评估汇总

#	初始事件	过程干扰	受到影响的过程参数	预防策略
1	冷却水控制失效	失去冷却功能，导致失控反应	— C. W. * 流量低； — 反应器温度高； — 反应器压力高	— 加入中止剂； — 反应器泄压(SIS)； — 压力安全阀(IPL)
2	搅拌器电机驱动失效	降低冷却效果，温度不均匀，导致失控反应	— 搅拌器电机电流低； — 反应器温度高； — 反应器压力高	—加入中止剂，使反应器“鼓泡”，从而停止失控反应； — 反应器泄压(SIS)； — 压力安全阀(IPL)
3	大面积停电(UPS仪表电源正常供电)	失去搅拌功能，导致失控反应	— 搅拌电机停止 — 冷却水流量低 — 反应器压力高 — 反应器温度高	—加入中止剂，使反应器“鼓泡”，从而停止失控反应； — 反应器泄压(SIS)； — 压力安全阀(IPL)
4	泵断电导致冷却水泵停止运行	失去冷却功能，导致失控反应	— C. W. * 流量低； — 反应器温度高； — 反应器压力高	— 泵可由蒸汽驱动； — 加入中止剂； — 反应器泄压(SIS)； — 压力安全阀(IPL)
5	批料配方错误—使用了两倍充装量的引发剂	引发剂浓度高会导致失控反应	— 反应器压力高； — 反应器温度高	— 加入中止剂； — 反应器泄压(SIS)； — 压力安全阀(IPL)
6	控制系统故障，导致反应器过量充装	温度上升，反应器充满液体，可能会导致反应器出现液压损坏和 VCM泄漏	— 充装液位高； — 充装重量大； — 反应器压力高	—将液位和重量与配方进行比较； — 反应器泄压(SIS)； — 压力安全阀(IPL)
7	温度控制失效导致在蒸汽加热过程中过热	高温导致失控反应	— 反应器高压； — 反应器高温	— 加入中止剂； — 反应器泄压(SIS)； — 压力安全阀(IPL)
8	反应器搅拌器密封失效	密封失效可能会导致危险的 VCM烟气泄漏	— 反应器密封处高压； —反应区域内的烟气探测	—环绕反应器密封四周加强额外通风； —通过高密封压力来实现反应器减压(SIS)
* C. W. 代表冷却水。				

作为上述危险识别的结果，PHA小组给出了如下建议 。

a) 实现用于处理失控反应场景的以下 SIS预防策略：

- 如果出现高温或高压条件，操作员有足够的时间远程添加中止剂 。

注 ：对于表 F. 6 中的第 2项和第 3项来说，加入中止剂之后，需要使反应器“鼓泡”，以便将中止剂混合至反应物质中，因为搅拌器不工作 。

- 如果这并未使失控停止，“高-高”温度或“高-高”压力 SIF将打开紧急泄压排放阀，以实现安全可控 。

b) 对于那些由于搅拌器不工作而发生的失控(表 F. 6 中的第 2 项和第 3 项)，除上文“a)”中建议外，还需要增加以下保护：

- 搅拌丧失(电流低)将通过报警提示操作员，加入中止剂后，需要使反应器“鼓泡”，以便将中止剂混合到反应物质中 。
- 根据上文“a)”中的建议，紧急减压 SIF是控制失控的备用功能 。

c) 冷却水流量低或无冷却水流量问题由上文 a) 建议中的保护功能控制 。 如果冷却水流量低是由于水泵失电造成的，则操作员会收到低流量报警，从而打开水泵的蒸汽驱动 。

d) 反应器过量充装水或 VCM 可能会导致溢出，并且可能会导致反应器出现液压过压损坏 。 如果称重传感器或反应器液位超过 BPCS内这一 批料添加步骤的“高”限，则需通过防止该批料受热而避免这一 问题 。作为备用，通过“高-高”反应器压力 SIF触发紧急泄压排放阀动作 。

e) 反应器内搅拌器密封失效会导致 VCM 的危险泄漏 。 为了避免这 一 问题，建议在检测到搅拌器密封高压时触发紧急泄压 SIF。

f) 由于中止剂系统在控制失控反应方面非常重要，因此小组也建议在 BPCS中使用保证中止剂不中断的联锁 。如果中止剂罐的液位低，或者如果该罐上的氮封压力低，则 BPCS联锁不允许将 VCM充装到反应器中 。

F. 9. 2 步骤 F.2:安全功能分配

表 F. 7 给出了在安全功能分配中关键因素的概述 。

表 F. 7 SIS安全生命周期— 方框 2

概述					
安全生命周期阶段或活动		目标	GB/T 21109. 1— 2022的要求章节或小节	输入	输出
GB/T 21109. 1— 2022 的图 7, 方框 2	将安全功能分配给保护层	将安全功能分配到保护层，并为每个 SIF分配相应的 SIL	9	要求的 SIF和相关安全完整性要求的描述	安全要求分配的描述(见 GB/T 21109. 1— 2022的第 9章)

F. 10 SIF安全完整性等级确定

利用所提出的 SIF清单，开展 PHA小组会议，使用保护层分析(LOPA)方法，以便为每个 SIF确定所要求的 SIL。关于 LOPA方法的描述，请参阅IEC61511-3:2016的附录 F。CCPS/AIChE《保护层分析 简化的过程风险评估》(2001)中给出了附加指南 。

F. 11 保护层分析(LOPA)应用实例

F. 11说明了将危险评估资料(表 F. 6)中的数据转换到 LOPA(表 F. 9) 。

以下给出 LOPA场景描述 。

— 事件 1:冷却水控制失效

这个场景会触发可能导致反应器灾难性破裂的失控反应 。此事件影响判定为“大范围的”,根据表 F. 8 注 1讨论的内容,该单一场景的可容忍频率为 10^{-5}/年 。控制系统中的若干失效都可能会造成这一 问题,操作经验表明,这类问题大约每 10 年发生 一 次 。符合表 F. 6 的保护措施为加入中止剂,但失控反应对于操作人员来说太快了,无法对报警做出响应 。这一保护层不包括在风险降低中 。 由于该区域通常会被占用,因此假设人员可能会受到此事件的影响 。PSV 的有效性预计仅为 90%,因为在这一运行中,堵塞是常见的问题 。 由于 PSV之间共用泄压管线,因此考虑为一个独立保护层 。这将导致中间事件的可能性为 10^{-2}/年 。 根据此例中所用的保守假设,只有 PSV具有成为 IPL 的资格 。PHA小组审核了所有的过程安全风险问题,并确定 SIF是合适的 。如表 F. 9所示,这要求一个 SIL3的 SIF。

注 :提供 PSV 的目的是符合压力容器标准要求,但如 LOPA所示(利用表 F. 8 的公司风险准则),这些为不足以满足此场景风险目标的保护措施 。这 一 注释对于此例中的所有 LOPA场景来说都是合适的 。

— 事件 2:搅拌器电机驱动失效

此场景会触发与事件# 1类似的失控反应,除此之外,由于搅拌停止,因此加入中止剂时需要增加使反应器“鼓泡”的附加步骤(F. 8)来停止失控反应 。再说,这 一 失控的速度如此之快,操作人员也许不能做出响应,因此操作人员不会采取任何风险降低措施来响应报警 。控制系统或搅拌器本身的几个失效都会造成此类问题,操作经验表明,此类问题大约每 10 年发生一次 。SIFS 1是这一事件唯一有效的 SIF,它需要 SIL3。

— 事件 3:大面积停电

尽管这一 问题与事件 F. 2具有明显的差异,SIFSIL选择与事件 F. 2 的结果类似 。

— 事件 4:冷却水泵电力失效

事件 4 中的问题与事件 1 中的问题类似 。通过启动蒸汽透平驱动水泵或加入中止剂,操作人员干预可以停止这种失控 。尽管操作人员动作被认为是非常有效的,由于操作人员的可用性问题,没有给予风险降低的可信度 。表 F. 9 内所示的分析得出 SIFS-1 为 SIL3。

— 事件 5:引发剂的双倍充装

这一 问题会导致非常剧烈的失控反应,即使冷却水正在运行,热量和压力都会快速上升 。升压速度如此之快,以致于不能有效地测量温度并触发 SIF。设计 PSV 和泄压 SIF的 目 的是安全地控制这一失控反应 。 由于设计和规程中的安全特性,这 一 问题的发生需要可能性非常低的失效组合,因此选用初始事件为中等可能性 10^{-1}。 中等可能性 、一个非 SIS IPL 以及“大范围的”严重性导致 SIFS-2 为 SIL3。

— 事件 6: 由控制系统失效导致反应器过度充装

这一 问题的影响是反应器液体压力过压,从而导致法兰垫片炸开或类似的泄漏事件 。 由于每年使用大量批料,而且它们的配方各有不同,因此判定这 一 可能性为中等(10^{-1}/年) 。小组判定操作人员响应 BPCS液 位 和 称 重 报 警 的 有 效 性 为 90% (10^{-1}),因 为 这 些 报 警 位 于 单 独 的 BPCS控制器中 。安全阀和泄压 SIS 对这 一 问题都会有作用 。严重性等级为“严重” 、中等的触发事件可能性以及两个非 SIS IPL表明 SIL1适用于泄压 SIF。 即使在此需要 SIL1 SIF,根据事件 5 的要求,最终将 SIFS-2 确定为 SIL3。

— 事件 7:加热过程中的温度控制失效—批料过热

此事件会导致与事件 1类似的失控反应 。 除不考虑温度变送器适用于这 一 事件的风险降低外,事件的影响和保护方面与事件 1类似 。在加热过程中,操作人员有时间添加中止剂从而防止失控 。然而,由于温度传感器用于控制,它可能是触发这种危险的一部分原因 。 因此操作人员对高温报警的响应可能不会成为这一事件的 IPL。需要将 SIFS-1设计成 SIL3,这已经在事件 1做出了要求 。

— 事件 8:搅拌器密封失效

如果该密封失效,用于这一反应器的特殊密封设计可以将 VCM 泄漏限制为小流量 。所提供

的现场通风足以将这一火灾和爆炸风险降至最低 。PHA小组将严重性判定为“严重的”,并确定现场通风的有效性为 90%(10^{-1}) 。 由于没有 IPL,严重性最终定为“严重的”,而且发生可能性高大 ,根据表 F. 9,定级为 SIL2恰当 。

F. 12 可容忍风险准则

表 F. 8 给出了用于本例的可容许风险准则 。

这些准则是针对特定公司的 。在定义必要的安全功能时 ,每个公司需采用自己的风险准则 ,并与当地监管机构的要求一致 。表 F. 9 由过程危险分析小组编制和审批 ,见 F. 2。

表 F. 8 容许风险分级

严重性	定义	可容忍频率 (事件数/年) (见注 1)
大范围的	导致一人或多人死亡或者造成不可逆的健康影响	10^{-4}
严重的	多个医疗处理情况伤害;1个或 2 个受限工作日情况或损失工作日情况或中等健康影响情况	10^{-3}
轻微的	轻微伤害或可恢复的健康影响	10^{-2}

注 1: 所示的可容忍频率为所有危险的总风险 。将每个 LOPA场景的可容忍频率设为比多个危险的频率低 一 个数量级(即将“大范围的”严重性的每个场景分配 10^{-5}的可容忍频率)。对于此例来说,这一方法是可以接受的 ,因为人员通常不会处于运行区域 ,日常的操作人员巡检(每次巡检 一 个人) 成为人员暴露在与这 一 操作相关的危险中的主要原因 。

注 2: 表 F. 8 的数据为公司标准 。

注 3: 此例中的公司是在英国和美国均有经营业务的公司。对于在英国执行的项目,可能会运用额外的风险准则 。英国健康与安全执行局(HSE)的观点是需要将有害事件的风险降低至任何进 一 步的风险降低成本将高于所获得的利益为止。 参考书目:《降低风险,保护人员》,HSE, ISBN 号:07176-2151-0, 出版年份,2001年;www.hsebooks.co.uk;IEC61511-3。

表 F. 9 VCM 反应器示例 :基于完整性等级的 LOPA

#	1	2	3	4	5			6	7	8	9	10	11	12
	影响事件	严重性等级/可容忍频率	初始原因	初始频率事件数/年	保护层			附加减轻措施	中间事件频率事件数/年	IPL的数量	是否需要 SIF	SIF完整性等级	已减轻事件频率事件数/年	注释 (SIF ID)
					过程设计	BPCS	报警等							
1	反应器破裂	E 10^{-5}	冷却水控制失效	10^{-1}	无	无	无	PSV 10^{-1}	10^{-2}	1 (PSV)	是	3 (泄压) 10^{-3}	10^{-5}	S-1
2	反应器破裂	E 10^{-5}	搅拌器电机驱动失效	10	无	无	无	PSV 10^{-1}	10^{-2}	1 (PSV)	是	3 (泄压) 10^{-3}	10^{-5}	S-1

表 F. 9 VCM 反应器示例 :基于完整性等级的 LOPA (续)

#	1	2	3	4	5			6	7	8	9	10	11	12
	影响事件	严重性等级/可容忍频率	初始原因	初始频率事件数/年	保护层			附加减轻措施	中间事件频率事件数/年	IPL的数量	是否需要SIF	SIF完整性等级	已减轻事件频率事件数/年	注释(SIF ID)
					过程设计	BPCS	报警等							
3	反应器破裂	E 10^{-5}	大面积失电力	10	无	无	无	PSV 10^{-1}	10^{-2}	1 (PSV)	是	3 (泄压) 10^{-3}	10^{-5}	S-1
4	反应器破裂	E 10^{-5}	冷却水泵电力失效	10	无	无	无	PSV 10^{-1}	10^{-2}	1 (PSV)	是	3 (泄压) 10^{-3}	10^{-5}	S-1
5	反应器破裂	E 10^{-5}	引发剂的双倍充装	10	无	无	无	PSV 10^{-1}	10^{-2}	1 (PSV)	是	3 (泄压) 10^{-3}	10^{-5}	S-2
6	反应器破损液体压力过压	S 10^{-4}	反应器过量充装，控制系统失效	10	无	无	液位(400 LSH)和称重传感器(300 WTH)报警 10^{-1}	PSV 10^{-1}	10^{-2}	1 (PSV)	是	3 (泄压) 10^{-3} (要求 SIL 1)	10^{-6} (要求 10^{-4})	S-2
7	反应器破裂	E 10^{-5}	温度控制失效加入过量蒸汽	10	无	无	无	PSV 10^{-1}	10^{-2}	1 (PSV)	是	3 (泄压) 10^{-3}	10^{-5}	S-1
8	VCM泄漏	S 10^{-4}	搅拌器密封失效	10	反应器密封处现场通风 10^{-1}	无	无	无	10^{-2}	0	是	2 (泄压) 10^{-2}	10^{-4}	S-3

严重性等级 E— 大范围的;S— 严重的;M— 轻微的(见表 F. 8);可能性值单位为事件数/年;其他数值为概率 。

为了简单起见，此例并不考虑反应器在 100%时间内未运行的情况，也未考虑这三台反应器中都存在危险这一事实 。

完成 LOPA后，将场景 1~场景 5 和场景 7 的已减轻事件可能性相加 。 总频率 6×10^{-5}满足表 F. 8 中所示公司对“大范围的”事件可允许频率为 10^{-4} 的准则 。 场景 6 和场景 8 的已减轻事件总频率为 1.01×10^{-4}，满足公司关于“严重的”事件可允许频率为 10^{-3} 的准则 。

F. 13 步骤 F.3:SIS安全要求规范

F. 13. 1 概述

表 F. 10 SIS安全生命周期— 方框 3

概述					
安全生命周期阶段或活动		目标	GB/T 21109. 1— 2022的要求章节或小节	输入	输出
GB/T 21109. 1— 2022 的图 7，方框 3	SISSRS	为了达到要求的功能安全，根据要求的 SIF 及其相应的安全完整性规定每个 SIS 的要求	10	安全要求的分配描述(见 GB/T 21109. 1— 2022的第 9章)	SIS安全要求；AP 安全要求

此 SRS示例中的信息可能包含在单个文件中，也可能包含在一组文件中 。 以下要求仅适用于本示例 。

F. 13. 2 输入要求

表 F. 11 中的 SIF及其相应的 SIL的信息为步骤 2 的输出，用于编制 SRS。

表 F. 11 安全仪表功能和 SIL

标识符	监测的过程变量	SIL
S-1	反应器高压和高温	3
S-2	反应器高压	3
S-3	搅拌器密封高压	2

BPCS执行有序启动和正常停车的操作功能 。这些功能不包括在本示例中 。

PHA小组已识别出堵塞是该应用中的一个潜在问题 。 在设计 SIS时，设计小组需要考虑到这一点 。

未识别出对 SIS设计产生影响的监管要求 。

F. 13. 3 安全功能要求

表F. 12列出了每个 SIF 的安全状态，并显示了过程输入与输出之间的功能关系，包括所要求的逻辑 。

表 F. 12 SIF的 I/O 功能关系

SIF #	SIL	传感器	描述	最终元件的安全状态
S-1	3	100PT 100PT1 100TT	如果反应器压力超过 0. 86 MPa或反应器温度超过 93. 3 ℃	打开 100PV 打开 100PV1
S-2	3	100PT 100PT1	如果反应器压力超过 0. 86MPa	打开 100PV 打开 100PV1
S-3	2	200PT	如果密封压力大于 0. 06895MPa	打开 100PV 打开 100PV1

表 F. 13显示了 SIS的过程仪表输入 、跳闸点 、正常运行范围以及运行极限 。

表 F. 13 SIS传感器、正常运行范围 & 跳闸点

标记	校准范围	正常运行范围	预跳闸报警		跳闸点	
100PT	0~1. 378MPa	0.4134 MPa~0.689MPa	0. 7924 MPa	上升	0. 8613 MPa	上升
100PT1	0~1. 378MPa	0.4134 MPa~0.689MPa	0. 7924 MPa	上升	0. 8613 MPa	上升
100PT	0~121 ℃	51 ℃~79℃	82 ℃	上升	93. 3 ℃	上升
200PT	0~0. 3445 MPa	0~0. 1378 MPa	0. 0345 MPa	上升	0. 0689 MPa	上升

所有的 SIF均设计为失电跳闸动作 。

当最终元件失去能量时 ,它们将按表 F. 9 的定义进入其安全状态 。 为满足架构要求和 PFDavg要求 ,对最终元件进行表决(1oo2) 。

每个 SIF的响应时间为一分钟或更少是足够的 ,除非另有说明 。

SIS使用经过IEC 61508评估的变送器和逻辑解算器。 经过评估的变送器也满足以往使用的要求 。

PHA小组的审查表明 , 当多个安全过程状态同时发生时 ,没有任何组合会产生一个单独的危险 。

变送器的系统性能力为 SC2,而逻辑解算器系统性能力为 SC3。

S-1 的变送器采用 1oo3表决 ,而 S-2 的变送器采用 1oo2表决 , 以满足架构和 PFDavg要求 。

BPCS的 HMI将作为 SIS的主要人机界面使用 。所有的报警显示功能将在 BPCSHMI中实现 ,无需使用硬接线报警 。工程/维护接口将置于具有安保措施的位置 。

HMI丧失时 ,操作员可以使用安装在控制台上的停车按钮 。该控制按钮用于启动 一 系列动作 ,使过程以有序的方式进入安全状态 。该停车按钮同时作为 SIS和 BPCS逻辑解算器的离散输入 ,并通过BPCS加入中止剂 。

PHA小组对所选 SIS逻辑解算器的安全手册进行了审查 ,确定了不需要在独立于逻辑解算器的情况下手动驱动安全阀 。基于该审查以及快速过程泄压的不良后果 ,SRS中将不包括对直接手动驱动的要求 。见逻辑图(图 F. 11) 。

由于这是一个批处理操作 , 当在 SIS中检测到故障时停止过程运行 。 即不允许过程在 SIS处于降级模式时运行 。

为了尽量避免 SIS触发停车 ,需为操作人员响应的预跳闸报警分配最高的优先级 。

SIS所有跳闸的复位均是手动的 。手动复位开关位于控制室的操作台 。

由于这是一个批处理操作,并且使用了良好的控制系统工程实践，因此无需关注误跳闸率 。

针对系统性 AP故障,提供了“镜像”(BPCS中对 SIS应用逻辑的功能性复制) 。普遍认为“镜像”会提高误跳闸率,但对于此例中的批处理过程来说,无需关注误跳闸 。

诊断检测到现场设备和 HMI故障会阻止开车,但当批处理过程运行时,仅提供报警 。

当 SIS停止过程时,所有 BPCS控制回路将被置于手动状态,并且输出被置于安全状态 。

需监测每个 SIS回路(例如,I/O、通信 、诊断),以确保它们在 SIS启动之前处于励磁状态 。

需自动检查每台变送器，以确保在 SIS启动之前不存在坏值(例如,低于 4 mA) 。

运行模式包括充装 、反应和卸料 。在每个模式中,SIS的所有功能都需运行 。

未提供任何超驰 、抑制或旁路 。

对于 SIS在重大事故事件中保持可用并无特殊要求 。

F. 13. 4 安全完整性要求

表 F. 9 中规定了每个 SIF所要求的 SIL。

为达到所要求 SIL,硬件要求如下：

- 逻辑解算器经 IEC 61508评估,为 SC3(即设备的 PFD_{avg}处于 0. 001与 0. 0001 之间)；
- 基于对 GB/T 20438的符合性和用户批准,选择传感器和最终元件(见 ISA TR 84. 00. 04—第1部分)；
- 所有最终元件设有位置传感器,并进行检查，以确保阀门位置与逻辑指令一致 。

为达到所要求 SIL,硬件要求如下：

- 逻辑解算器提供的诊断;
- SIS和 BPCS二者均检查其中所有输入传感器的上限和下限;
- 在 SIS和 BPCS二者中均对 100PT和 100PT1做比较诊断;
- BPCS中的“镜像”。

反应器每年停车两次进行离线维护和安全联锁测试 。需以相同频率测试 LOPA 中确定的提供风险降低的所有保护层 。注意：由于该示例是批处理操作，因此，为满足 目标 PFD_{avg}，必要时可采用更高的频率测试某些 SIS设备(例如,可在每批生产开始前测试放空阀) 。 目前,F. 16(“SIF设备参数”)中所述的 SIL验证计算表明,不需要使用更高的测试频率 。然而,如果操作经验显示 SIF设备的实际失效率高于 PFD_{avg}计算中的假设值,则可以对某些设备实施更高频率的测试 。

所有 SIF均由 UPS供电，以减少误跳闸 。 由于这是批处理过程，因此没有对避免误跳闸提出附加要求 。

通过以下措施将共因失效降至最低：

- 为冗余压力变送器提供单独的引压管;
- 为冗余排放阀提供单独的管线;
- 确保在表 7事件 6 中声明为 IPL的报警完全独立于 SIF(即 BPCS的控制功能 、报警功能和“镜像”功能采用单独的 DCS控制器)；
- 应用如 F. 18和 F. 19所述的良好工程实践(例如,接地 、浪涌保护 、电源 、多样性)；
- 针对人因(例如,配置 、校准 、测试),由不同的人员进行检查和批准 。

F. 14 功能描述和概念设计

F. 14阐述了如何根据安全功能要求和安全完整性要求进行 SIF架构设计 、每个 SIF的 SIL验证以及 SISAP的开发 。

F. 14. 1 反应器系统逻辑的说明

在 SIS中,实施了三个自动 SIF(S-1 到 S-3)：

- SIFS-1和S-2防止反应器出现高温/高压失控,因为这一反应为放热反应,并且高温会造成高压;
- 如果压力变送器 100PT或 100PT1超过 0. 8613 MPa,或者温度变送器 100TT超过 93. 3 ℃,则安全功能 S-1会打开反应器的排放阀 。

当添加双倍量的引发剂或者反应器过量充装时,升压会非常迅速,因此设置 SIF S-2 以防止上述事件发生 。 由于温度变送器响应稍慢,可能无法检测到这 一 非常快速的事件,因此温度变送器 100TT不包括在 PFD_{avg}计算中 。如果 100PT或 100PT1超过 0. 8613 MPa,排放阀打开 。

此应用使用了完全相同的智能压力变送器,因此需考虑会导致两台变送器同时失效的系统性错误的概率 。SIS和 BPCS逻辑解算器中都提供了诊断,以检测超上限 、超下限或两个变送器的数值偏差 。在 PFD_{avg}计算中,考虑了 F. 16所述的诊断覆盖率 。

设置 SIFS-3, 当 200PT测得密封压力超过 0. 0689 MPa时,打开排放阀 100PV 和 100PV1。

由于场景 1~场景 8 的触发原因对相同 SIF的设备提出要求,因此需对这些要求加和,以确定每个SIF的操作模式 。在此例中,这些要求加和为 0. 8 次/年,即对该 SIF的要求率低于 1 次/年 。 因此,每个SIF均为低要求模式 。关于要求操作模式与连续操作模式的指南,见 ISA TR84.00.04:2015和A. 9. 2. 3。

表 F. 14 因果图

反应器因果图(表格形式)						
原因				结果		
安全功能编号	传感器/输入	描述	跳闸设定值	最终设备	动作	说明
S-1	100PT 100PT1	反应器压力“或”	>0. 8613 MPa	100PV	打开	反应器泄压
	100TT	反应器温度	>93. 3 ℃	100PV1	打开	反应器泄压
S-2	100PT 100PT1	反应器高压	>0. 8613 MPa	100PV 100PV1	打开 打开	反应器泄压
S-3	200PT	反应器密封压力	>0. 0689 MPa	100PV 100PV1	打开 打开	反应器泄压

F. 15 SIL验证计算

考虑上述功能和完整性要求后,为每个 SIF绘制示意图(即如图 F. 4、图 F. 6 和图 F. 8 所示的气泡图),以便:

- 阐述如何满足功能要求和完整性要求;
- 说明 SIF架构如何满足 SIL要求;
- 给出每个 SIF子系统(传感器子系统 、逻辑解算器子系统 、最终元件子系统)的 PFD_{avg};
- 提供 SIS架构的配置依据;
- 提供 SIFPFD_{avg}计算的基础 。

然后,采用商业软件,基于气泡图绘制每个 SIF的故障树 。故障树分析软件的输出是 SIF的 PFD_{avg}(见图 F. 5、图 F. 7 和图 F. 9) 。此时,将计算得到的 PFD_{avg}与所要求的 PFD_{avg}(见表 F. 9 第 10栏)进行比较;当计算得到的 PFD_{avg}不能满足表 F. 7 的要求时,需相应地更改概念设计 。

表 F. 15中列出了每种类型的 SIF设备及其可靠性参数 。这些参数来源于以往使用 、供应商数据和行业数据库,并重点关注来自现场的数据 。

平均无危险失效时间(MTTFd) :

表 F. 15 SIS设备的 MTTFd

紧急排放阀	60年
压力变送器	60年
RTD温度变送器	60年
电磁阀	35年
SIS逻辑解算器	2 500年

共因:

共因问题采用 F. 18所述技术进行处理 。通过在每个 SIF的故障树中加入共因因子来处理残余的共因失效 。这些因子基于工厂经验 。对于阀门和电磁阀,共因失效估算为未检测到的危险失效总和的1%;对于变送器,共因失效估算为未检测到的危险失效总和的 2%[即,对于变送器,共因失效造成的未检测到的危险失效率等于 0. 02×(1/60);对于阀门,共因失效造成的未检测到的危险失效率等于 0. 01×(1/60);对于电磁阀,共因失效造成的未检测到的危险失效率等于 0. 01×(1/35)] 。

系统性故障:

SIS逻辑解算器的系统性能力为 SC 3,它与硬件的失效 、架构要求(故障裕度) 和嵌入式软件相关 。需注意在逻辑解算器的评估中,未考虑 AP 的系统性失效 。 系统性逻辑解算器的 AP 的失效问题通过在 BPCS内 “镜像” 逻辑来处理(见图 F. 4、图 F. 6 和图 F. 8 的气泡图) 。BPCS用于减少 SISAP的系统性失效;但是,BPCS硬件对 PFD_{avg}的影响未包括在每个 SIF的故障树分析中 。

注 1: 除实施 GB/T 21109. 1— 2022第 12章中要求的技术外,还使用了上述技术 。

压力和温度变送器为智能设备,含有可编程(固定编程语言) 特性,基于对 IEC 61508的符合性,其系统性能力为 SC 2。这些变送器用于 SIL3应用(即 SIF S-1&SIF S-2) 。 为了处理系统性失效,每个SIL3 SIF实施了多种技术 :

- 对于 SIFS-1,设备选型时基于以往使用性能,且在设计中采用了多样性(温度和压力)以及诊断(见 F. 14. 1, “反应器系统逻辑的说明”),以确保系统性软件错误处于与 SIL3应用相称的水平 。
- 对于 SIFS-2,通过实施以往使用分析(见下面的注释) 、故障树分析(见图 F. 7)和采用诊断措施来确保变送器中的系统性软件失效处于与 SIL3应用相称的水平 。

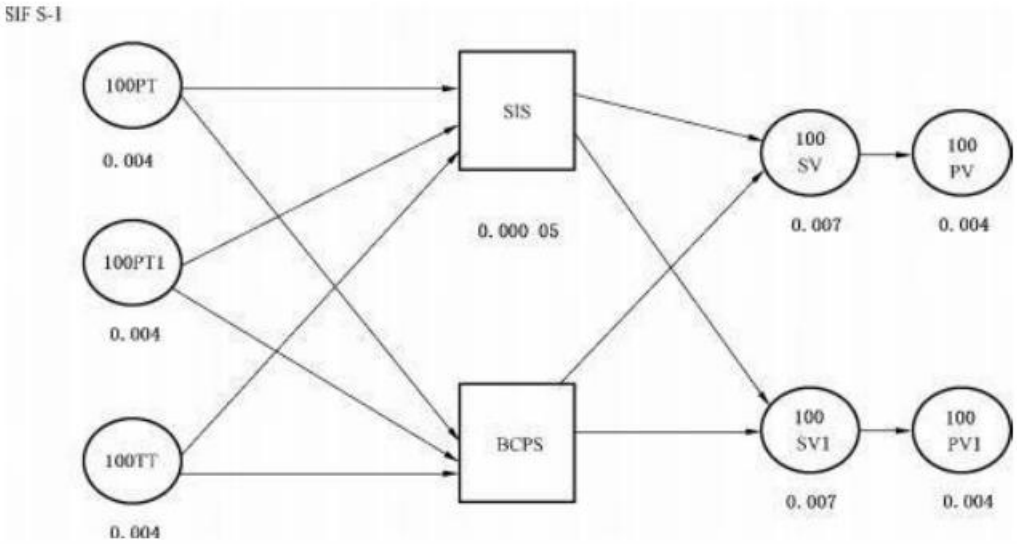
注 2: 根据以往使用数据,小组估计,变送器中总共因失效的 2%是由于软件故障造成的 。 图 F. 7 内所示的故障树说明了软件故障是如何在 SIFS-2 的 PFD_{avg}计算中起作用的 。如果没有充分的以往使用数据可用,则可以使用替代方案,用户联系变送器制造商,使其保证开发嵌入式软件时所使用的技术符合 IEC 61508中给出的关于SIL3软件指南的要求 。

硬件故障裕度(HFT) :

对于 SIFS-1 和 SIFS-2,用于传感器和阀门的故障裕度基于 GB/T 21109. 1— 2022的表 6(SIL3) 。

对于 SIFS-3,用于传感器和阀门的故障裕度基于 GB/T 21109. 1— 2022的表 6(SIL2) 。

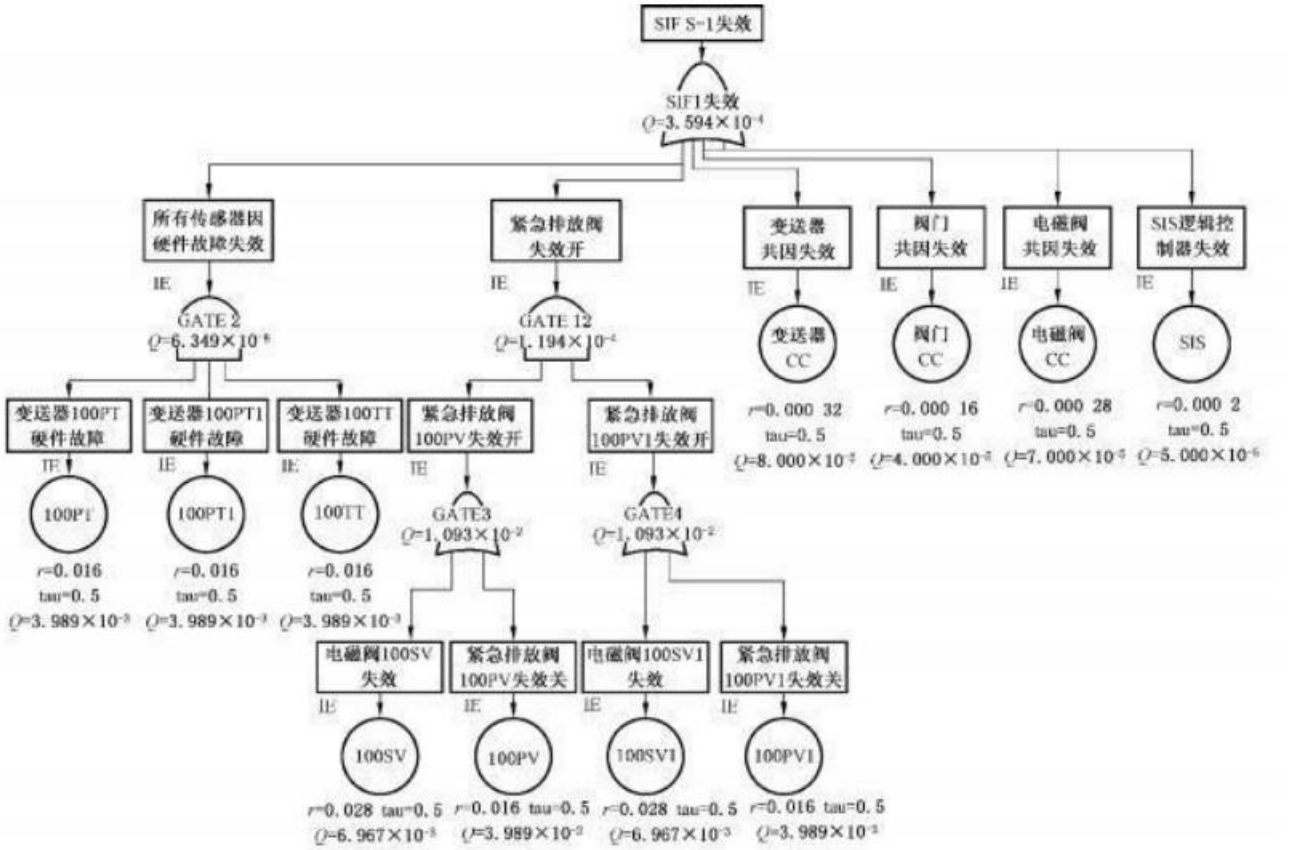
逻辑解算器按满足 IEC 61508(包括故障裕度)关于 SIL3应用的要求进行设计,并由第三方进行评估 。 因此,SIFS-1、SIFS-2 和 SIFS-3 的故障裕度满足了 IEC 61511的要求 。



项目#	修订版次 #	修订	修订人	审核人	批准人	日期	项 目 # YYYY 日期；
							制图人 :S. Bulk
							审核人 :V. May
							R. Brown
							批准人 :W. Burk
							图纸号 ： # XXXXX1

图 F. 4 显示每个 SIS设备 PFD_{avg}的 SIFS-1气泡图

故障树计算，见图 F. 5。



项目#	修订版次 #	修订	修订人	审核人	批准人	日期	项 目 # YYYY　　日期：
							制图人 :S. Bulk
							审核人 :V. May
							R. Brown
							批准人 :W. Burk
							图纸号 ： # XXXXX1

说明：

E — 使能事件；

Q — 不可用性(PFD_{avg})；

r — 失效率(失效/a)；

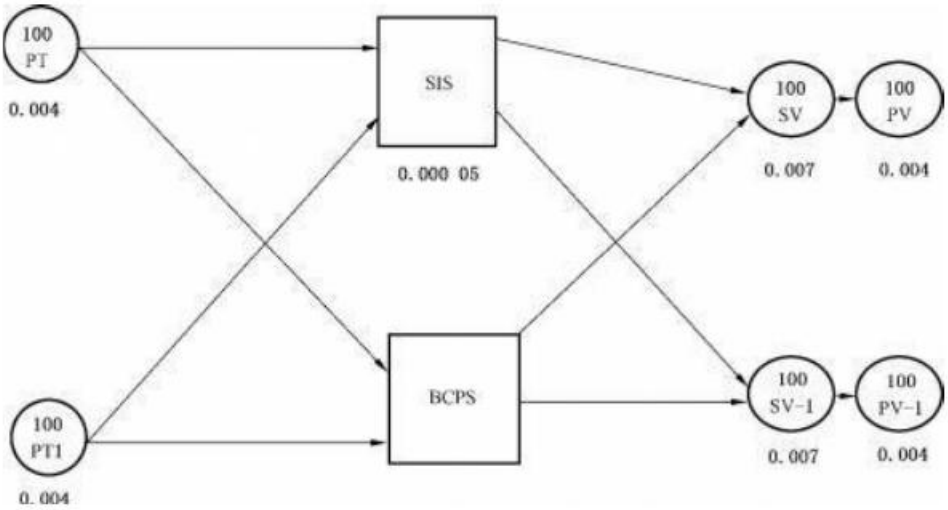
tau— 测试间隔(a)。

SIFS-1 的 PFD_{avg}约为 3.6×10^{-4}，因此满足 SIL3的要求。

图 F.5 S-1 故障树

SIFS- 2

如果反应器的压力高于 0.861 3 MPa，打开排放阀 100PV 和 100PV1。所要求的 SIL=3(表明 $PFD_{avg}=10^{-3}\sim10^{-4}$)。

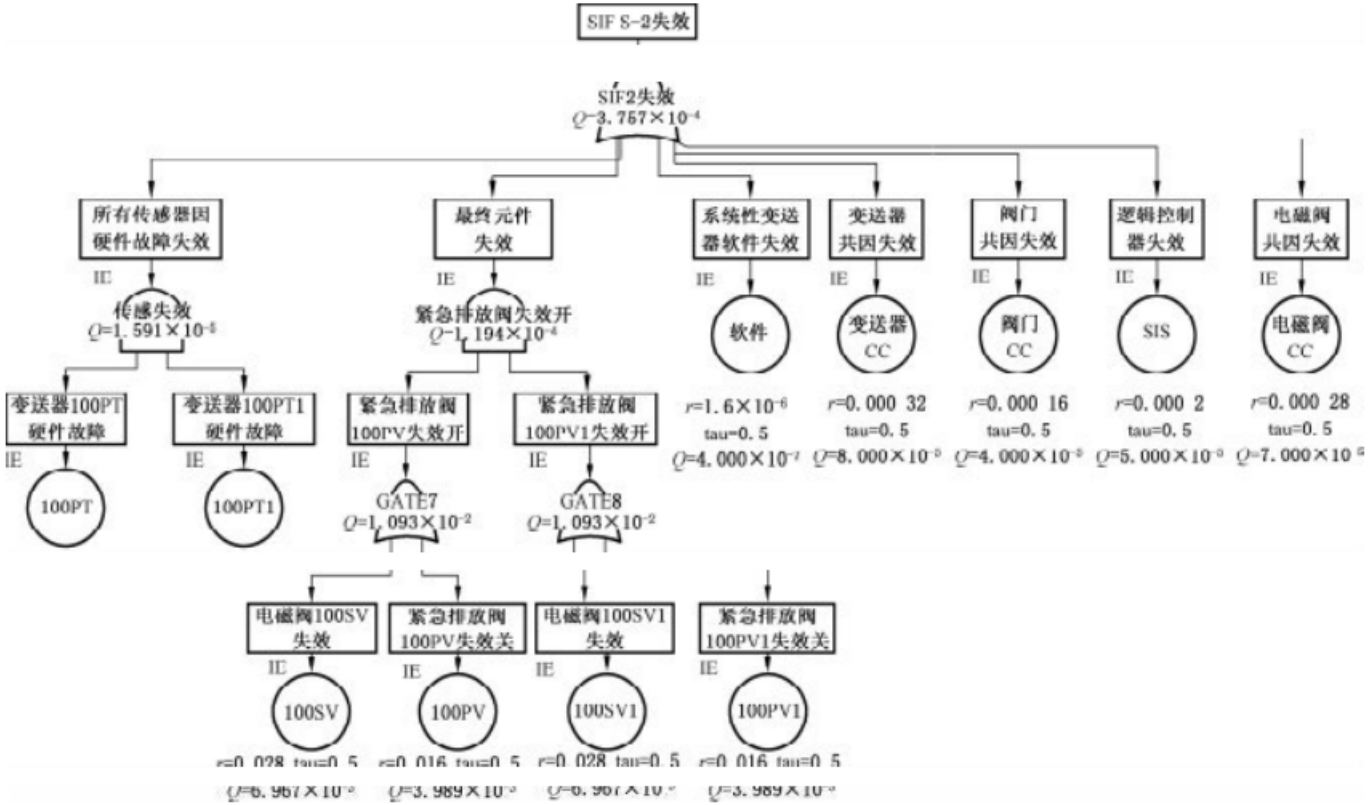


项 目 #	修订版次 #	修订	修订人	审核人	批准人	日期

项 目 # YYYY 日期；
制图人 :S. Bulk
审核人 :V. May
R. Brown
批准人 :W. Burk
图纸号 ： # XXXXX1

图 F. 6 显示每个 SIS设备 PFD_{avg}的 SIFS-2 气泡图

故障树计算，见图 F. 7。



项目#	修订版次 #	修订	修订人	审核人	批准人	日期

项 _目 _# _Y　　日期：
制图人：S. Bulk
审核人：V. May
R. Brown
批准人：W. Burk
图纸号 :# XXXXX1

说明：

E — 使能事件；

Q — 不可用性（PFD_{avg}）；

r — 失效率（失效/年）；

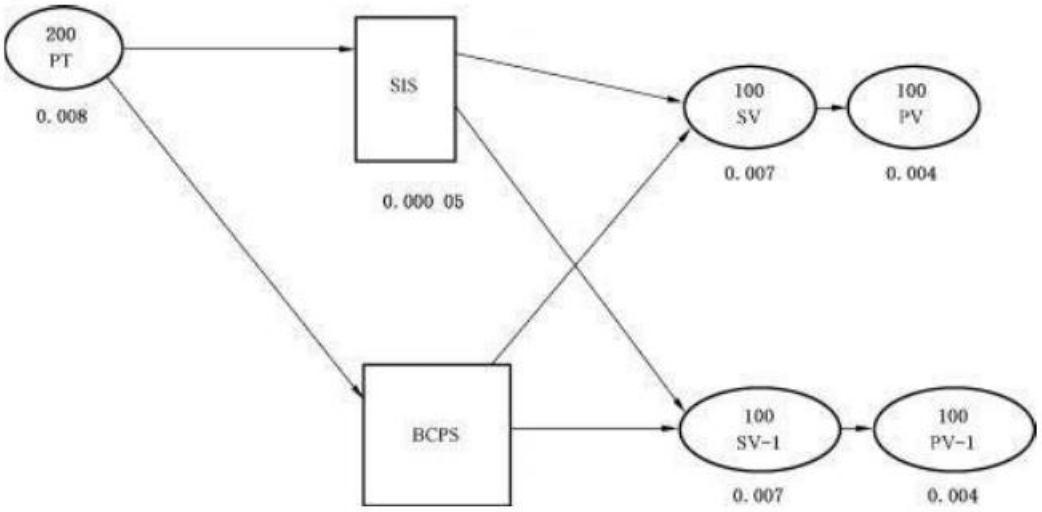
tau— 测试间隔（年）。

SIFS-2的 PFD_{avg} 约为 3.8x10^{-4}，因此满足 SIL3的要求 。

图 F.7　SIFS-2故障树

SIFS- 3

如果搅拌器密封压力大于 10psig,则打开 100PV 和 100PV-1。所要求的 SIL=2($PFD_{avg}=10^{-2}$ 至 10^{-3})。

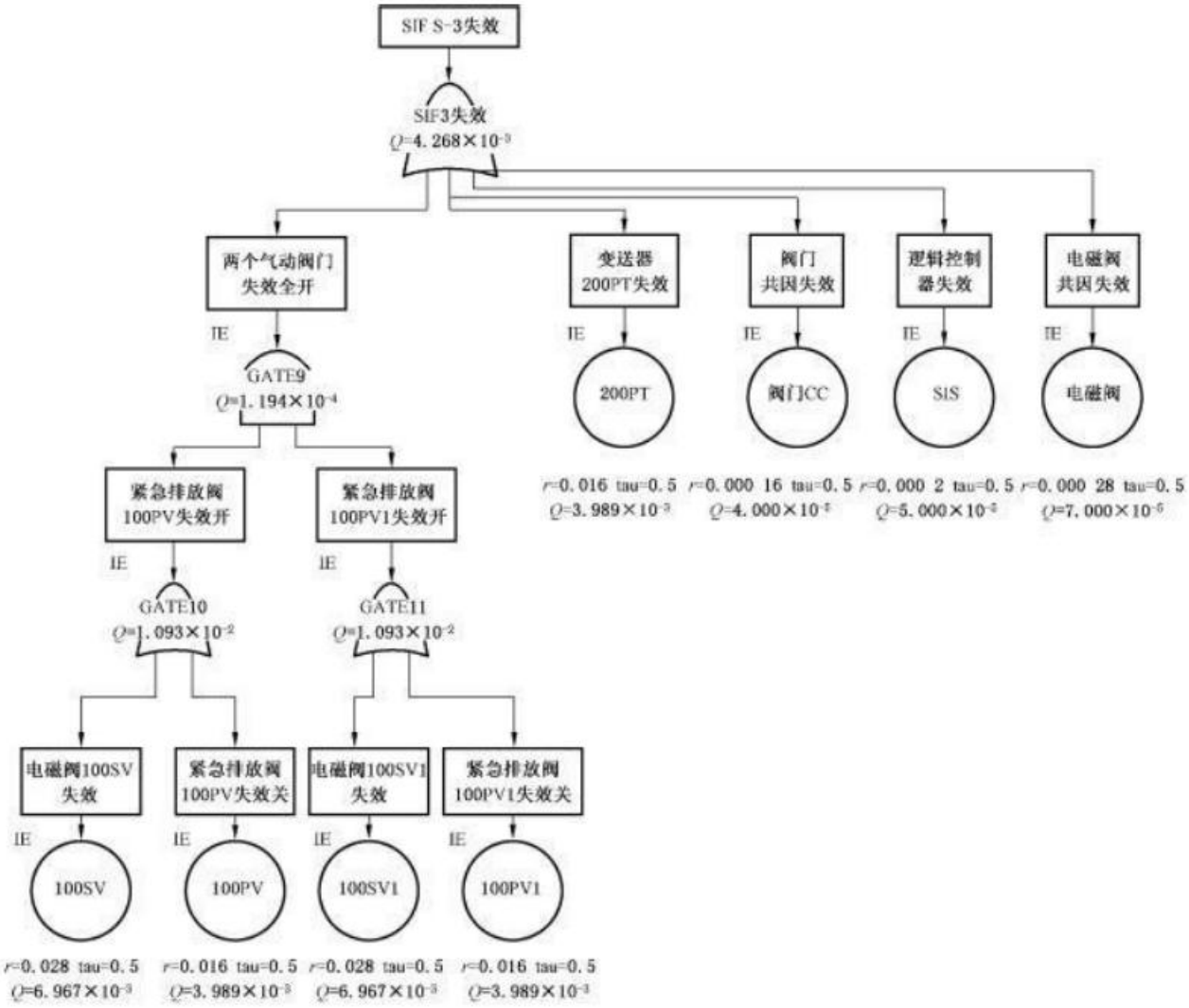


项 目 #	修订版次 #	修订	修订人	审核人	批准人	日期

项 目 # YYYY 日期;
制图人 :S. Bulk
审核人 :V. May
R. Brown
批准人 :W. Burk
图纸号 : # XXXXX1

图 F. 8 显示每个 SIS设备 PFD_{avg}的 SIFS-3 气泡图

故障树计算,见图 F. 9。



项目#	修订版次 #	修订	修订人	审核人	批准人	日期

项 目 # YYYY 日期;
制图人 :S. Bulk
审核人 :V. May
R. Brown
批准人 :W. Burk
图纸号 : # XXXXX1

说明：

E — 使能事件；

Q — 不可用性(PFD_{avg})；

r — 失效率(失效/年)；

tau— 测试间隔(年)。

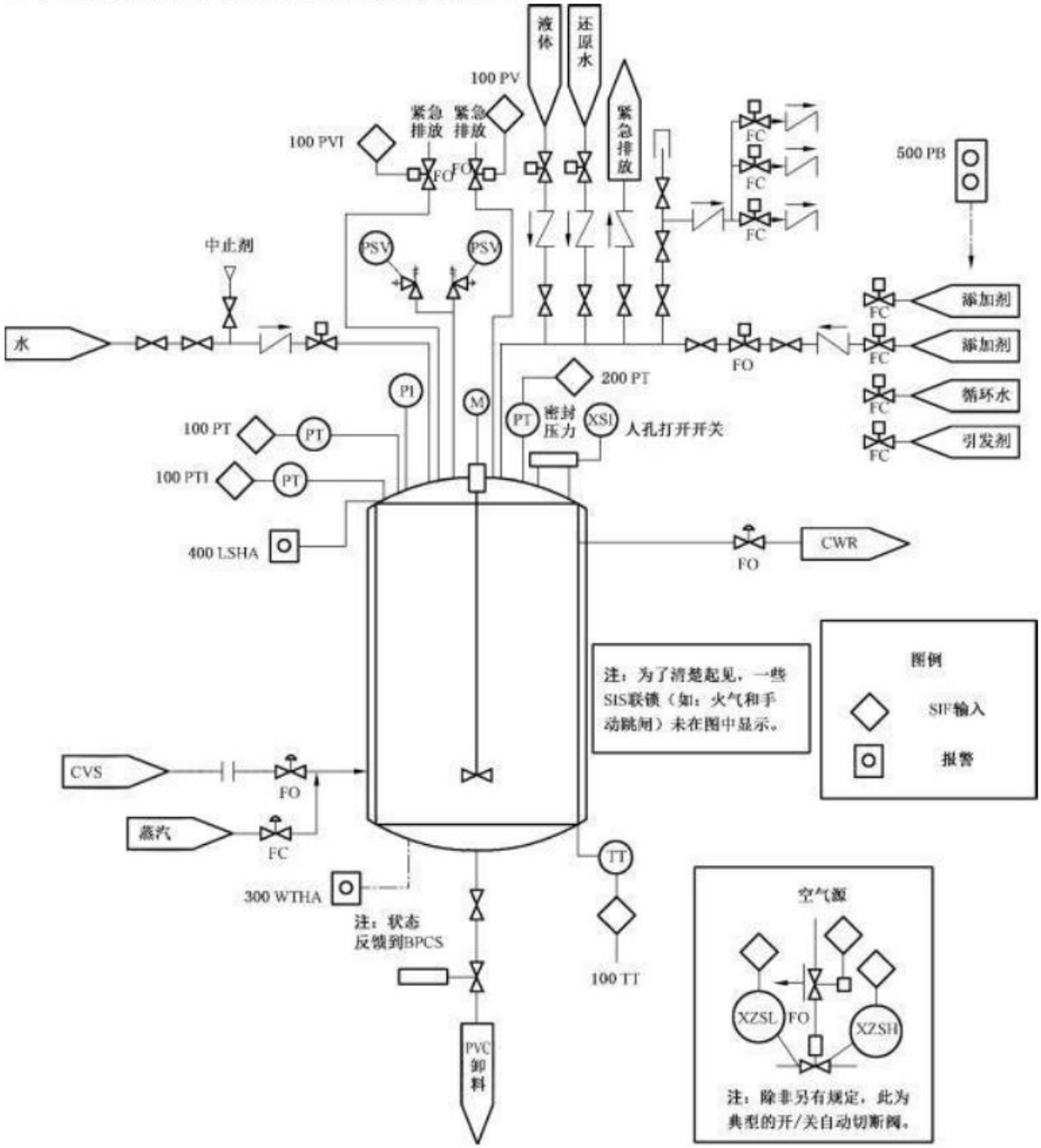
SIFS-3 的 PFD_{avg}约为 4.3×10^{-3}，因此满足 SIL2的要求 。

图 F. 9 SIFS-3 故障树

F. 16 应用程序要求

SRS[特别是逻辑说明(F. 14. 1) 、因果图(表 F. 14)和 P&I图(图 F. 10)]用于制定 AP要求 ,如梯形图中的说明(图 F. 11) 。

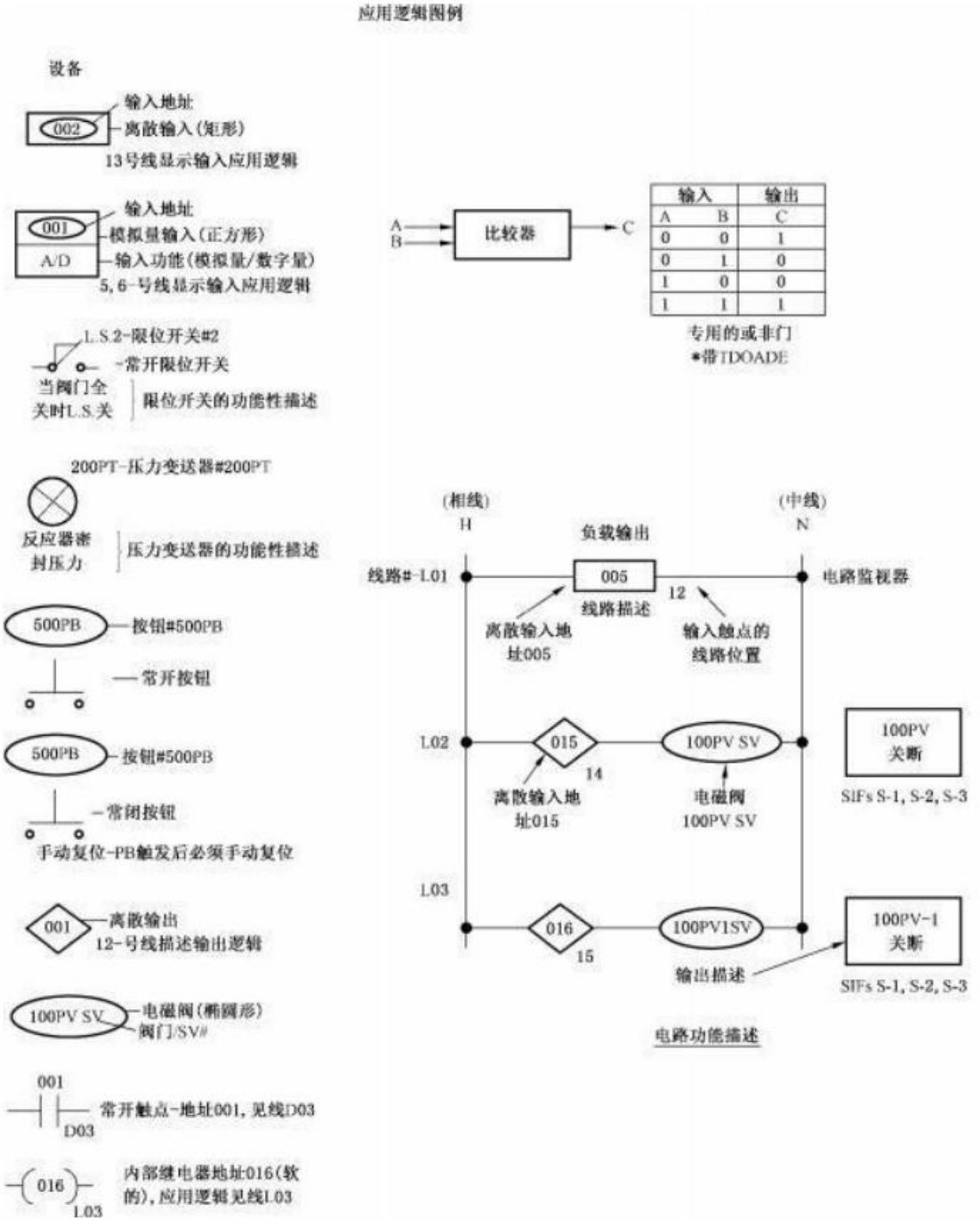
用于表示每个 SIF的功能要求的梯形图见图 F. 11中 。该梯形图也给出了电路的电压特性 、接地特性 、电路要求和诊断，以协助设计/编程人员开发 AP。



项目#	修订版次 #	修订	修订人	审核人	批准人	日期

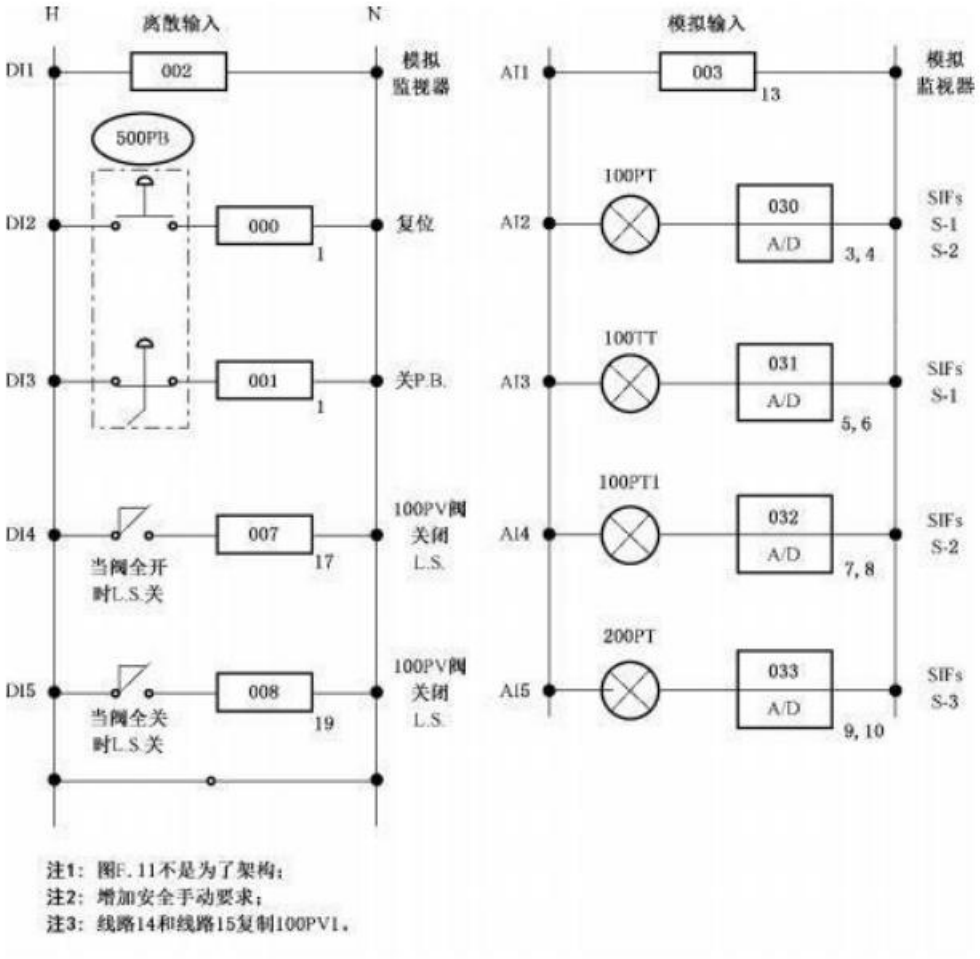
项 目 # YYYY　　日期：
制图人 :S. Bulk
审核人 :V. May
R. Brown
批准人 :W. Burk
图纸号 ：# XXXXX1

图 F. 10　PVC反应器单元 SIF的 P&ID



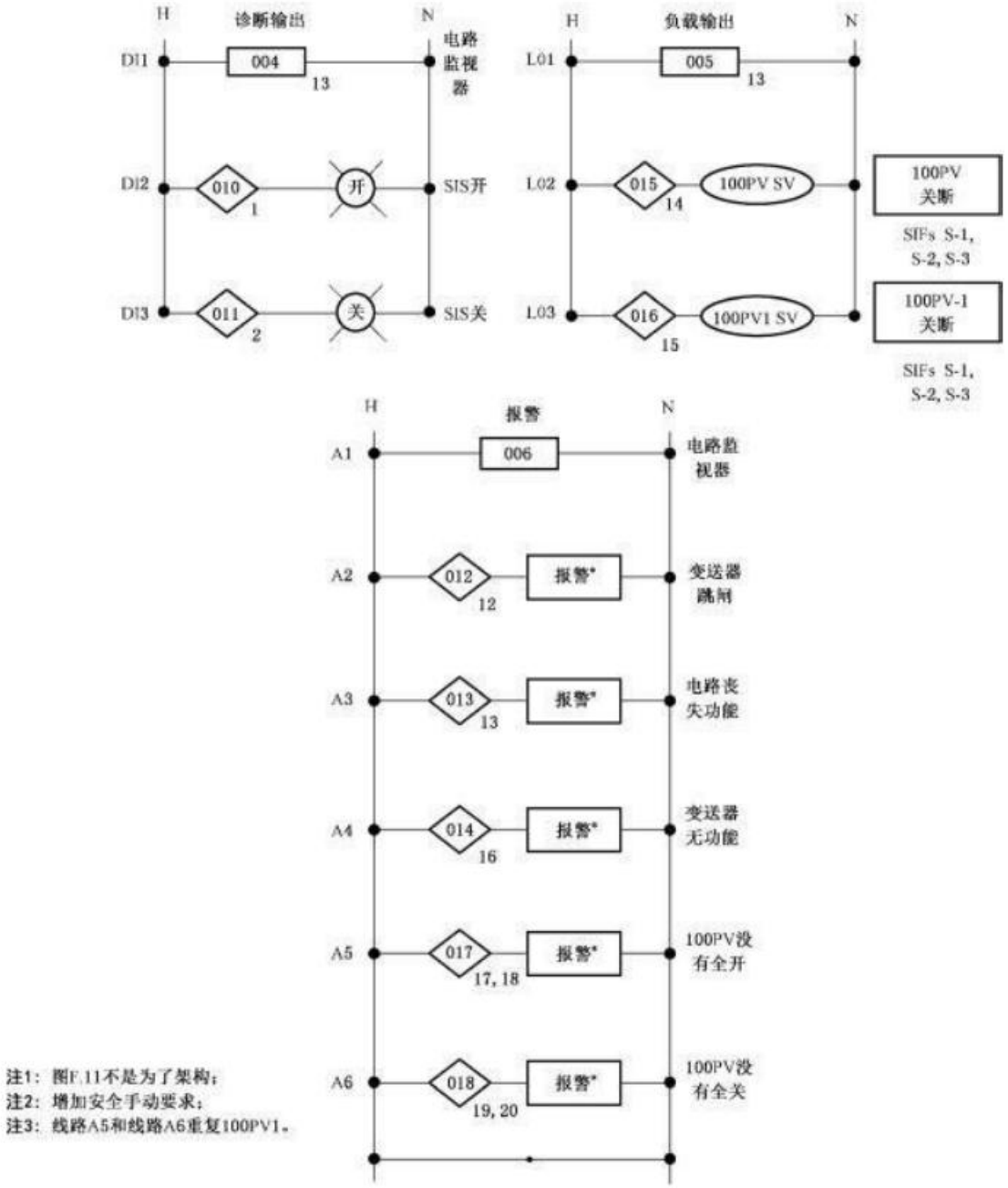
项目#	修订版次 #	修订	修订人	审核人	批准人	日期	项目 # YYYY	日期；
							制图人 :S. Bulk	
							审核人 :V. May	
							R. Brown	
							批准人 :W. Burk	
							图纸号：# XXXXX1	

图 F.11 图例(第 1 页/共 5 页)



项目#	修订版次 #	修订	修订人	审核人	批准人	日期	项目 # YYYY　　日期；
							制图人 :S. Bulk
							审核人 :V. May
							R. Brown
							批准人 :W. Burk
							图纸号 ：# XXXXX1

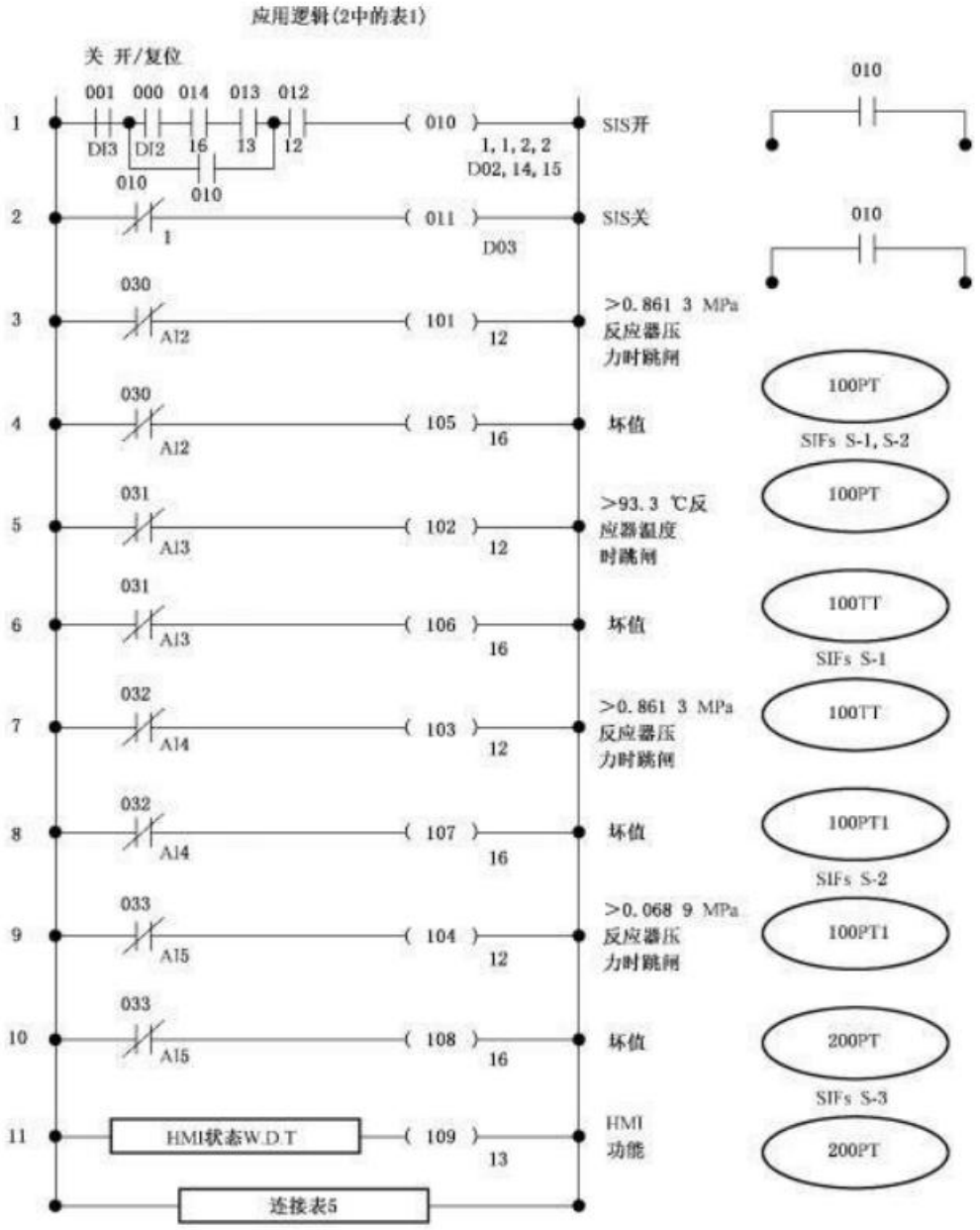
图 F.11　图例(第 2 页/共 5 页)



注1：图F.11不是为了架构；
注2：增加安全手动要求；
注3：线路A5和线路A6重复100PV1。

项目#	修订版次 #	修订	修订人	审核人	批准人	日期	项目# YYYY 日期；
							制图人 :S. Bulk
							审核人 :V. May
							R. Brown
							批准人 :W. Burk
							图纸号：# XXXXX1

图 F.11 图例(第 3 页/共 5 页)

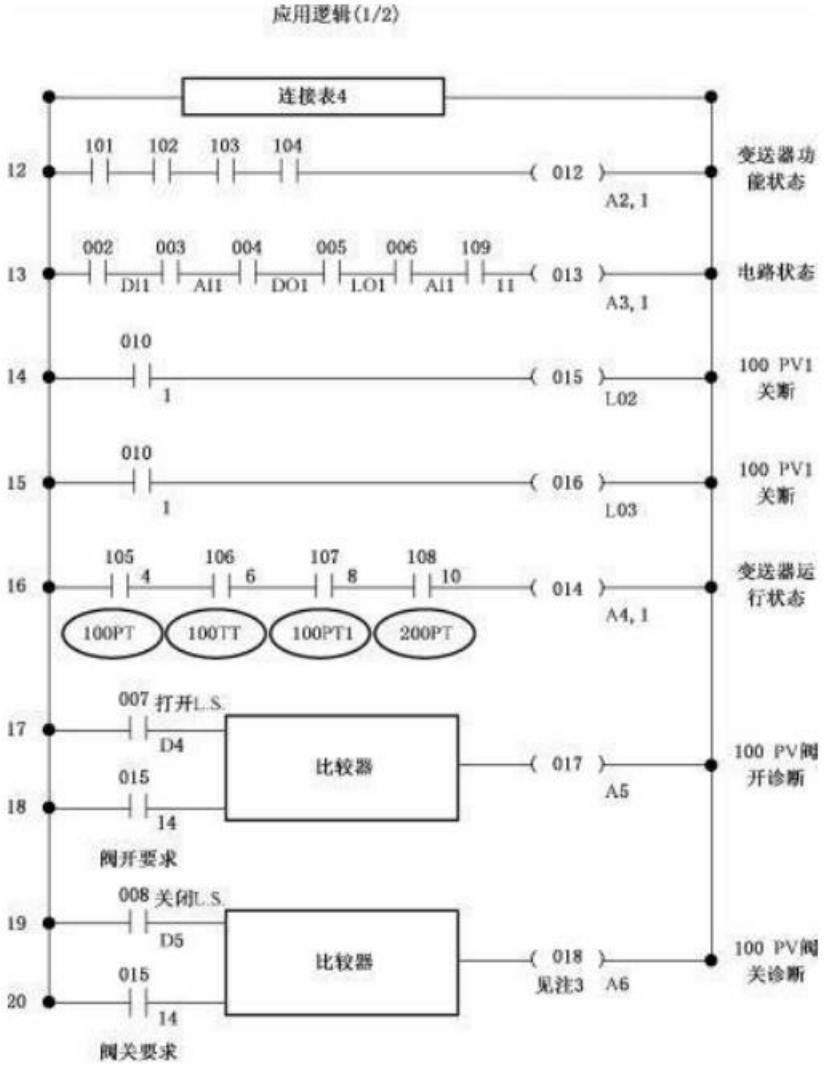


注1：图F.11不是为了架构；
注2：增加安全手动要求。

项 目 #	修订版次 #	修订	修订人	审核人	批准人	日期

项 目 # YYYY　　日期；
制图人 :S. Bulk
审核人 :V. May
R. Brown
批准人 :W. Burk
图纸号 : # XXXXX1

图 F.11 图例(第 4 页/共 5 页)



注1：图F.11不是为了架构；
注2：增加安全手动要求；
注3：线路17、线路18、线路19和线路20复制100PV1。

项目#	修订版次 #	修订	修订人	审核人	批准人	日期	项目 # YYYY　　日期：
							制图人 :S. Bulk
							审核人 :V. May
							R. Brown
							批准人 :W. Burk
							图纸号 : # XXXXX1

图 F.11　图例(第 5 页/共 5 页)

F. 17　步骤 F.4:SIS安全生命周期

表 F. 16　SIS安全生命周期— 方框 4

概述					
安全生命周期阶段或活动		目标	GB/T 21109. 1— 2022 的要求章节或小节	输入	输出
GB/T 21109. 1— 2022 的图 7,方框 4	SIS设 计 和 工程	设计 SIS 以 满 足 SIF 及其相应的安全完整性的要求	11和 12. 4	SIS安全要求; AP安全要求	符合 SIS安 全 要 求的 SIS设计; SIS 集 成 测 试 计划

表 F. 16给出了 SIS设计和工程的目标 、输入以及相关的章节和条款参考 。

F. 18　技术和设备选择

F. 18. 1　概述

F. 18列出了本例中选择技术和设备时所采用的关键参数 。

a)　工厂 PHA小组批准 SIS使用的所有设备;
b)　工厂熟悉的低复杂性设备;
c)　有文件来源的系统性能力;
d)　与工厂人员能力/经验相符的维护和测试准则;
e)　基于现有工厂准则的操作人员/维护接 口 ;
f)　按项目预估和时间节点编制的成本和进度表;
g)　将 BPCS用于 AP多样性(“镜像”);
h)　所选择的所有技术之前已经用于工厂(即以往使用),并且工厂维护人员能很好地理解这些技术;
i)　有文件记录的各设备(包括数据源)的失效模式和失效率;
j)　对现场电磁干扰的抗扰能力;
k)　对各设备提供振动保护(例如 ,振动导致电路板接口松动 、设备和接线失效等) 。

F. 18. 2　逻辑解算器

逻辑解算器参数包括 :

a)　应用 F. 18. 1 “概述” 中的各项;
b)　逻辑解算器按 IEC 61508进行评估 ,具备系统性能力 SC 3。应用编程使用有限可变语言(即梯形图逻辑) ;
c)　所有逻辑解算器设备位于厂房的控制室中;
d)　所有的 SIF的过程安全时间足够长 ,典型的 PLC响应时间是合适的;
e)　在选择安全逻辑解算器的过程中 ,考虑工厂运行和维护经验(即以往使用) ;
f)　与 BPCS适当集成 。

F. 18. 3　传感器

除阀门位置开关使用接近开关(利用非接触特性)外 ,采用变送器代替离散开关 。

在 SIS和 BPCS逻辑解算器中对变送器辅以对超范围和输出值不当进行诊断 。

变送器的失效率数据基于 IEC 61508评估或符合 IEC 61508的系统性能力 ,并假设遵循了良好的安装实践 。

每台传感器均设有单独的引压管 。

所采用的变送器均为可编程(智能)设备 ,并具有以下特性 :

a) 诊断 、远程访问校准信息和在板设备描述特性 ,以更好地保证相应的设备已就位并处于正常运转状态 。

b) 限制访问校准调整的安全特性(例如 :写保护 、密码 、钥匙硬锁) ,以防不经意变更导致设备无法执行其安全功能 。

c) 适当的变送器刷新时间(即 ,过程变化到传感器输出响应之间的延时是可以接受的) 。

d) 需要时 ,变送器具有排液 、放空和测试连接能力 。

e) 变送器 4 mA~20mA 的输出信号直接连接至 SIS且并联至 BPCS。

F. 18. 4 最终元件

所采用的最终控制设备为电磁阀和紧急排放阀 。最终控制设备为失能跳闸 ,在失去气源或电源时进入安全状态(即紧急排放阀故障打开) 。

基于以往使用选用最终控制设备 。

F. 18. 5 电磁阀

电磁阀要求如下 :

a) H 级或 F级高温模压线圈 ,在连续通电的状态下具有更长的寿命(通常用于失电跳闸应用) ;

b) 电磁阀具有满足或超出所安装环境条件的高低工作温度额定值;

c) 阀门驱动器排放孔大小满足应用的时间要求(10秒以内的阀门响应时间是足够的) ;

d) 逻辑解算器输出值足够低 ,从而保证输出处于 “of” 模式时电磁阀会断开 。

电磁阀的平均危险失效时间(MTTFd)根据以下内容确定 :

1) 从实际操作经验(内部和外部)和供应商提供的数据中获得以往使用的信息;

2) 以往使用信息表明 ,在类似应用中使用 140个单位年的过程中 ,电磁阀出现了两次危险失效(阀门不排气) 。根据这一点 ,按 70%的置信下限(见 GB/T 21109. 1— 2022的 11. 9. 3 和11. 9.4中的注释和 TR84.00.04-1、TR84.00. 09)计算出的 MTTFd为 38. 7年 。在 PFD_{avg}计算中 ,选用 35年的 MTTFd。

F. 18. 6 紧急排放阀

当紧急排放阀失去动力源和操作信号时 ,需确保排放阀的动作符合功能安全要求 。基于上述以及所有不同失效动作要求的 PHA评估 ,紧急排放阀在以下情况下打开 :

a) 失电;

b) 失气;

c) SIS逻辑解算器或 BPCS逻辑解算器对电磁阀的打开信号 。

此外 ,紧急排放阀具有以下特性 :

1) 提供阀门实际位置的可视化指示 ,包括 :

- 通过阀杆位置指示器进行本地指示;
- 通过限位开关给出阀门开度位置的远程指示 。

2) 采用弹簧复位执行机构 。执行机构规格和失效安全弹簧设计的考虑包括了对最大关闭压力要求的合理分析 。

注 ：对于本过程应用 ,采用流体在阀芯下面流通的截止阀 。

对每个阀门的监控包括对阀门信号与阀门位置的对比 ,并辅以报警 。

F. 18. 7 调节阀

本例中考虑的 SIF不需要调节阀 。

F. 18. 8 旁路阀

经过 PHA小组的分析 ,确定不必使用旁路阀 。 因为批处理过程可提供离线维护机会 。 就这 一 问题 ,咨询了运行方和维护方 ,他们认可该做法 。

F. 18. 9 人机界面(HMI)

F. 18. 9. 1 概述

逻辑解算器接口功能设计为向 BPCS提供一个功能安全的接 口 ,用于“镜像”、操作员界面 、报警 、诊断和特定值的交换 。

在 BPCS的 SIS接口中 ,实现了以下几个方面的内容 ：

- 使用冗余 HMI控制台;
- 使用冗余通信链路;
- 为处理关键数据(例 如 送 往 BPCS操 作 员 控 制 台 的 所 有 数 据) 的 接 口 使 用 内 部 通 信 看 门 狗 计时器;
- 停车按钮(500PB)安装在其中一个 HMI控制台上 ,并配有塑料安全盖 ，以避免意外误碰停车 。

在操作员接口的设计过程中考虑的因素包括 ：

- 报警管理要求;
- 操作员响应的需要;
- 良好的人体工程学 。

只能通过 SIS工程师站 ,并采用合适的安防措施(F. 22) ,才能更改 SIS的 AP(包括跳闸设定值) 。

F. 18. 9. 2 报警管理

报警管理确保问题和危险通过报警优先级及时并以易于识别和理解的方式呈现给操作员 。报警优先级体现了现场的报警管理原则 。所实现的特性包括 ：

- 在 LOPA 中 采 信 的 用 于 风 险 降 低 的 报 警 具 有 最 高 的 优 先 级 。 这 些 报 警 (300WTHA 和 400LSHA)宜像 SIS一样 ，以每年两次的频率进行检查;
- 在 SIS动作之前引发操作员动作的预跳闸报警具有最高的优先级;
- 使用 BPCS操作员接口的特性区分不同优先级的报警;
- 使用预跳闸和跳闸报警帮助确定操作员响应要求;
- SIS诊断报警显示在 HMI的单独画面中 。

F. 18. 9. 3 操作员响应

操作员响应 HMI报警的能力需要实施以下方面 ：

- 使用事件顺序(SOE)记录 :BPCS的正常扫描时间给出了真实的首出报警功能;
- 使用预跳闸报警 :操作员可能会在发生跳闸之前采取纠正动作(例如添加中止剂以防止失控反应) 。在这些情况中 ,将发出预跳闸报警 。预跳闸报警和跳闸设定值考虑了过程动力学和传感器响应 。

F. 18. 9. 4 人因

“人因”针对接口设计参数,它会影响操作员对报警和状态信息有效识别并响应的能力 。设计因素包括:

- 颜色 、灯光 、类型 、形状 、开关尺寸以及开关位置等的一致性;
- 操作员停车开关(500PB)使用开关保护,从而降低意外操作的可能性;
- 操作员停车开关(拉起复位)的机械操作 。

F. 18. 10 隔离

F. 18. 10. 1 概述

F. 18. 10阐述了在每个 SIF的设计中固有的隔离过程 。

提供隔离的目的是减少共因故障,并便于解决可能由于意外变更而出现的安防问题 。这类问题可以使 SIS和 BPCS同时不可用 。为了解决上述问题,采用了与工厂培训和成功的以往使用经验 一 致的设计方案 。

F. 18. 10. 2 电源

SISI/O 电源与非 SIS电源电路的分离宜通过为 SIS仪表配电盘使用独立的配电变压器实现 。这可以预防与接地有关的共因故障。 进一步分开SIS电源,以确保冗余电源[即正常和不间断电源(UPS)]的线路实现物理分离,且划分支路分别向输入、逻辑解算器、I/O电源、负载输出和诊断输出供电 。

无需使用分离的电缆管道(例如 ,导管 、电缆槽和电线槽),因为已采用以下良好工程实践处理电磁兼容性(EMC)问题 :

- 最大电源等级(不大于 480V);
- 电缆/电缆通道/设备规范和间隔;
- 将电源和仪表信号线(即 4 mA~20mA)分到不同的电缆中;
- SIS设备的唯一标识(即颜色编码);
- SIS端子连接点的覆盖;
- 识别每根导线 、电缆 、电缆通道和连接点的计算机化布线程序 。

F. 19 共因和系统性失效

F. 19. 1 概述

F. 19. 2~F. 19. 19定义针对共因和系统性失效问题的设计考虑 。

避免共因失效的设计技术包括隔离 、冗余 、多样性和同行审查 。

用于避免出现系统性错误的技术包括同行审查 、使用具有良好以往使用跟踪记录的设计方法 、多样性以及比较诊断 。

F. 19. 2 多样性

通过使用不同的设备(SIS和 BPCS逻辑解算器) 、使用不同的设计执行同 一 功能(SISAP和 BPCS“镜像”) 、使用不同的嵌入式和 AP以及由不同程序员编程 ,从而实现多样性 。

F. 19. 3 规格书错误

通过熟悉所审核问题主题的人员进行同行审查 ,从而识别和纠正规范错误[例如 ,错误的环境温度

范围 、不正确的参数(例如 ,原本想要使用 0 °F时 ,却采用了 0 ℃) 、仪表使用不当材料] 。

F. 19. 4　硬件设计错误

通过使用符合以往使用准则(基于 IEC 61508评估 、或 IEC 61508符合性数据 、或工厂认可分析)的SIS设备，以应对硬件设计错误 。设计遵循公司的最佳实践 、每台认证设备的安全手册以及非认证设备的应用手册 ,并包括同行审查 。

F. 19. 5　软件设计错误

根据以往使用情况以及 IEC 61508评估或 IEC 61508符合性选用 PE设备 。BPCS中的 AP用于“镜像” SISAP,从而获得多样性嵌入式软件的好处 。

为了减少由于嵌入式软件故障造成的系统性失效 ，SIS和 BPCS中都组态有对两台压力传感器测量值的比较以及上下限检查 。

通过实施下列技术和措施 ,控制 AP系统性错误 ,包括：

- 对所有应用编程使用有限可变语言 ,除非可以采用固定可变编程(例如 ,基于 PE 的变送器 、基于 PE的操作台)；
- 所有涉及人员均能理解的逻辑文件编制方案(见图 F. 11) ,在 AP文档中嵌入了易懂的过程相关文件;
- 利用同行审查和仿真工具减少 AP设计错误;
- 采用“镜像”持续监测 AP性能并提供编程方式的多样性;
- 制造商的安全手册要求 。

F. 19. 6　环境过度应力

设施设计不考虑地震或飞机失事 ,但规定能承受 5 级飓风 。SIS所处的环境条件包括：

- 温度;
- 湿度;
- 污染物;
- 振动;
- 接地;
- 电源线路调节;
- 电磁兼容性(EMC) 。

F. 19. 7　温度

逻辑解算器 、I/O模块 、传感器和最终元件等 SIS设备会受到极端温度的不良影响 。 与温度相关的设计决定包括：

- 制造商规定的工作温度;
- 将设备置于温度偏离额定值不超过制造商规范的区域;
- 对室外设备的气象防护和温度控制;
- 使用集液包或排水管 ,或干燥仪表空气，以适当地降低由于结冰而导致失效的可能性;
- 需要时设置伴热 。

F. 19. 8　湿度

宜根据制造商的要求维持相对湿度(对于电子系统 ,通常低于 90%) 。为了减少较高湿度的不良影响(例如蒸汽、室外条件) ,宜通过保形涂层和“接触不粘”防潮剂来保护电子件 ,从而保证连接件之间的气密性。

F. 19. 9　污染物

为了避免潜在污染 ,宜提供以下措施 :

- 对环境充分地通风和防尘;
- 对腐蚀性大气环境 ,为 HVAC系统安装过滤器或提供吸附材料 ,并为所有其他的设备实现(空气)吹扫;
- 对于现场安装的电子设备 ,使用带吹扫的机柜和/或保形涂层 ,并对连接处设置保护 。

F. 19. 10　振动

建筑物会存在一定程度的振动 。 为了应对这 一 问题 ,所有的 SIS插入式设备(例如 “冰块式” 继电器 、I/O板)均设有闭锁设施 。SIS逻辑解算器柜利用振动隔离支架以尽可能减少从机柜到逻辑解算器之间的振动传递 。

F. 19. 11　接地

为便于使用可编程电子技术 ,采用以下接地设计 :

- 接地系统电阻低于 5 Ω;
- 使用 Ufer系统(基础)接地;
- 电气连续的建筑钢;
- 需要时 ,用铜导体代替建筑钢 “保护锥(coneofprotection)” 。

F. 19. 12　电源线路调节

电源线路调节设计的目的是为 SIS提供针对诸如断电 、雷电 、突降 、减弱 、停电 、浪涌和尖峰等电源线路异常 。

防雷由下列保护设备提供 :

- 与受保护设备的承受能力(例如短路 、过载)相协调;
- 位于适当的位置 , 以保护每个 SIS设备和保护锥 。

现有电力分配系统确实含有谐波 。设计 SIS电力分配系统以避免受到谐波的影响 。

SIS过载和短路保护具有以下特性 :

- 单独熔断每部分 I/O 电路 , 以限制该电路中故障的影响;
- 使支路熔断器与馈送支路的电路协调 ,从而尽可能降低由于低层级的故障导致更大部分 I/O 结构丧失功能的可能性 。

F. 19. 13　电磁兼容性(EMC)

电子和可编程电子系统使用了对电气噪声如电磁干扰(EMI)敏感的小电平信号 、数字电路 、微处理器 、存储芯片等 。在设计过程中 ,对人员通信系统如手持式双向无线电 、基站无线电 、手机 、个人电脑 、无线调制解调器和变频驱动器产生的 EMI进行了评价 。针对此问题 ,SIS设计实现了以下特性 :

a)　电子外壳为 SIS提供保护 ,避免受到外部(机柜外)噪声源的影响;

b)　电缆通道和电缆设计为 SIS提供保护 ,避免受到内部(机柜内)噪声源的影响;

c)　在需要时 ,提供噪声滤波器 。

其他 EMI降低技术包括 :

1)　金属外壳;

2)　金属屏障;

3)　电缆和电线屏蔽;

4） 双绞线;
5） 正确地接地;
6） 正确的设备安装位置;
7） 接线敷设远离 EMI源；
8） 隔离 。

SIS设备选用准则要求设备能承受工业环境中典型的 EMI等级 。通过以下方式实现 ：

- 根据适行标准(例如 IEC 61131,TUV)规定所设计 、搭建和测试的设备;
- 按制造商的安装指南安装设备 。

F. 19. 14 动力源

电力和仪表气源是维护 SIS的关键动力源 。其容量和设计的质量直接关系到其为 SIS提供服务的可用性 。不管如何设计 ,在 PHA过程中 ,假设部分的或所有的此类动力源会不可用 。

通过咨询电力和工厂人员(例如 ,动力室 、其他操作流程)，以确定现有动力源的可用性 。基于这些发现 ,动力源的设计具有提高可用性的特性 ,包括 ：

— 仪表气源

- 使用清洁 、干燥的仪表质量气源;
- 为最终控制设备提供足够的气动能力，以确保最终控制设备具有充足的运行时间;
- 气动通风口提供了防护 ,避免受到封堵 、污物 、虫类和结冻的影响;
- 确定气源和信号管路的长度和直径 ,要确保提供令人满意的性能 。

— 电力

- SIS逻辑解算器 、输入 、HMI和诊断输出使用冗余电源;
- 为马达荷载提供延时欠压保护(30个周期)；
- 后备电源具有与主电源相同的电源质量;
- 装备后备电源(例如 UPS) ,确保每个电源在维护时不会影响另一 电源的性能;
- SIS设计为在所有 SIS电路可用时方可允许启动 。

F. 19. 15 传感器

每台传感器均使用各自单独的引压管嘴，以尽可能减少共因失效 。

F. 19. 16 工艺腐蚀或污垢

该工艺因出现异常工艺条件而导致腐蚀的可能性有限 。它也是 一 个批处理过程 ,有助于在流程运行期间进行清理 。没有实施特别的设计要求 。

F. 19. 17 维护

维护组织参与了设计的规划 、验证和审批 。 因为与校准 、培训要求 、旁路和测试有关 ,维护组织特别留意了这些方面的设计 。

F. 19. 18 误操作敏感性

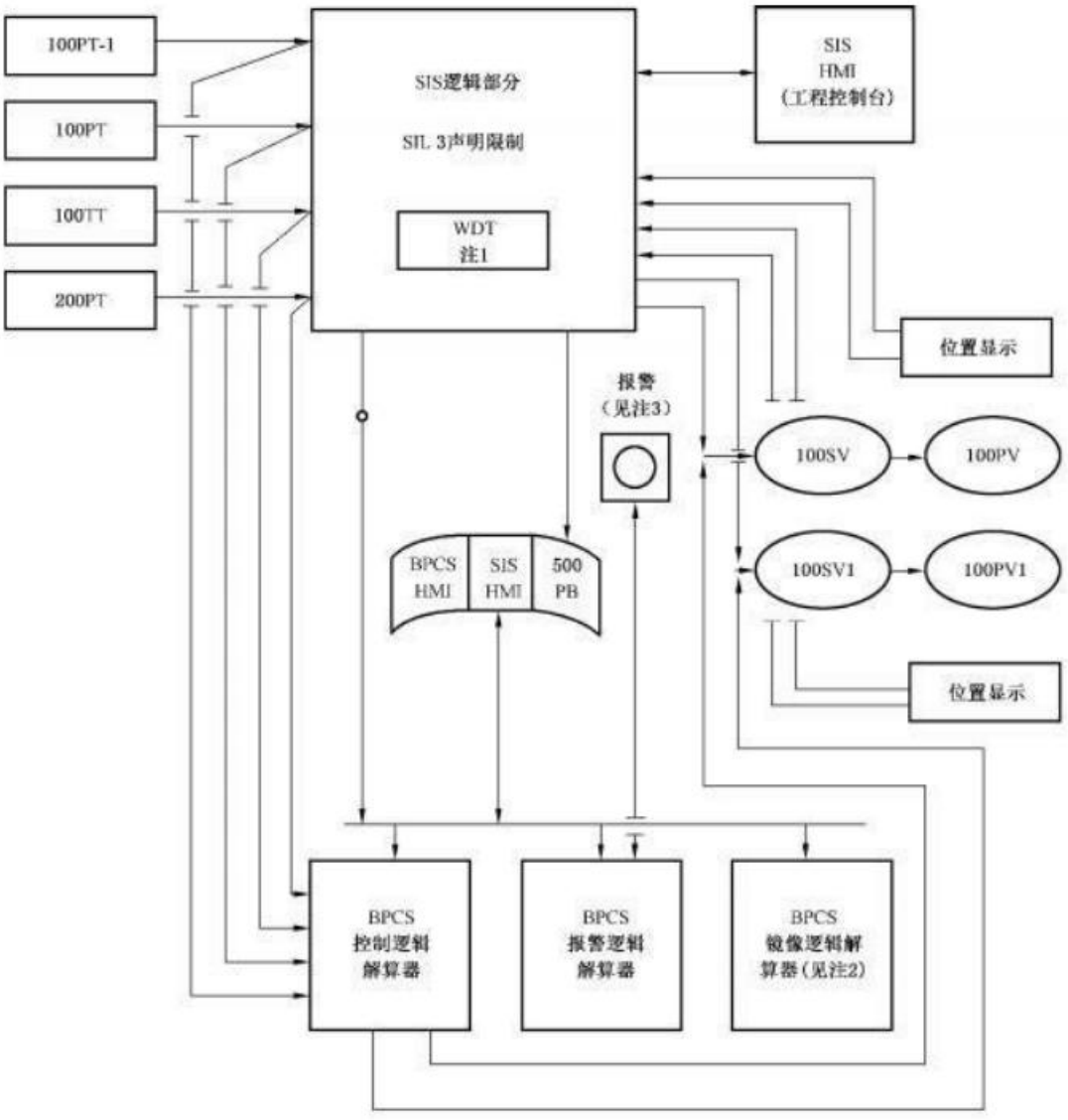
操作部门参与了设计的规划 、验证和审批 。特别关注了与以下方面有关的设计：简化操作规程 ,在生产运行中尽可能降低操作员干预要求 ,有适当的操作模式确保在关键时间区间内有能力终止批次生产 ,确保其满足过程需求的 AP测试，以及确认妥善处理了报警管理/HMI问题 。

F. 19. 19 SIS架构

下文讨论了 SIS架构 。 图 F. 12给出了 SIS架构 ,F. 19. 19的 目 的是给出 SIS架构及其与外部影响

因素(例如，BPCS、HMI、过程传感器和最终元件)之间的关系 。

BPCS与 SIS通过高速数据通信 。然而，安保强制要求对 SIS设定点的更改和对 SIS配置的更改只能通过专门的 SIS工程师站进行 。对 SIS设定点或配置进行更改时，SIS工程师站宜在控制室直接连接到 SIS。



注1：由通信WDT提供的到SIS HMI的通信连接确保SIS HMA在运行周期内可用。
注2：SIS应用软件的镜像。
注3：重量&液位报警[300 WTA & 400LSA(见图F. 11)]。

项 目 #	修订版次 #	修订	修订人	审核人	批准人	日期	项 目 # YYYY　　日期：
							制图人 :S. Bulk
							审核人 :V. May
							R. Brown
							批准人 :W. Burk
							图纸号 ： # XXXXX1

图 F. 12　VCM 反应器的 SIS

F. 20　SIS应用程序设计特性

AP文件结合了足以详细说明每个符号的作用 、每个 SIF的作用以及每个符号与其 SIF之间的关系的注释 。这些注释足够完整 ,有助于工程和维护人员理解 AP功能并在 AP 内导航 。

F. 21　配线实践

良好的配线实践对于确保达到想要的 SIS可用性是必不可少的 。 以下是该 SIS中实现的配线实践的清单 。

— 各电路不共用中线或 DC公共回线 ,从而尽可能降低 :

- 中线或公共回线电势升高或断开时 ，电路意外中断的可能性;
- 接地形成环路和接线错误的可能性;
- 额外的(10%的余量 ,20%的空间)分支电路 。

— I/O保险丝特性包括 :

- 利用单独熔断的 I/O 电路以更好地隔离故障 ,并尽可能降低可能的共因失效的影响;
- 使用隔离式 I/O;
- 在要求时以及在尽可能减少移除卡件的情况下 ,使用外部保险丝(即位于 PLC外部的 I/O保险丝) ;
- 将保险丝座接线端子(设有一体化保险丝座/分离杆)作为维护用途的断开手段使用 。

—使用抗 EMC透明玻璃以允许对诊断信息(例如 ,I/O灯)的可视化访问 。

— 为 SIS设置内部(即 SIS逻辑解算器机柜内)照明和扭锁式插座 ,从而避免插入感性设备 。

— 当 SIS终端位于非 SIS端子附近时 ,可以识别出 SIS终端 。

— 在需要的情况下 ,使用双绞线来尽可能减少磁场和共因噪声 。

F. 22　安防

通过防止对任何 SIS功能或设备(包括逻辑解算器 、应用逻辑 、用户接口 、传感器和最终元件) 进行未经授权或无意的修改 ,在 SIS设计方面采取的安防措施维持了安全完整性 。对于那些更难以控制物理访问的设备(例如 ,接口装置)来说 ,宜使用管理规程 。

所实现的一些基本的安防手段为 :

- 含有访问原因的书面审批;
- 含有要求访问的人员的书面审批;
- 在允许访问之前 ,确定所需的培训和/或对系统的熟悉程度;
- 确定访问系统的人员 、在何种情况下访问以及执行什么工作;这包括了用于控制维护旁路所需的规程 。

SIS的便于进行访问控制的特性 。此类设计特性的例子包括 :

- 通过鲜明的颜色位号来清楚地识别 SIS设备;
- SIS和 BPCS设备的物理分离(使其更易于用键锁来实现对相关外壳的安保) ;
- 使用异构的技术(通常需要不同的维护接 口) 。

使用基于 PES的 SIS引入了额外的安保问题 ，因为更改应用逻辑相对容易 。对于这些系统来说 ，实现了附加的特性 ,包括 :

- 限制访问维护/工程接 口 ;
- 制定管理方针/规程 ,定义在正常操作过程中可将维护接口连接到系统的条件;
- 在工程师站中使用病毒检测软件以及适当的程序和文件处理规程 ,从而有助于避免嵌入式和/或应用逻辑被损坏;

- 使用跟踪应用逻辑版本并且可以确定(更改成为事实后) 何时更改 、何人更改以及更改的组成部分的 SIS工具软件;
- 严禁 SIS或 BPCS对外连接至互联网或电话线 。

F. 23 步骤 F.5:SIS安装、调试、确认

表 F. 17 SIS安全生命周期— 方框 5

概述					
安全生命周期阶段或活动		目标	GB/T 21109. 1— 2022 的要求章节或小节	输入	输出
GB/T 21109. 1— 2022的图 7,方框 5	SIS安装 、调试和确认	集成和测试 SIS 根据要求的 SIF及其相应的安全完整性,确认 SIS在各方面都满足安全要求	12.3、14、15	SIS设计 ; SIS集成测试计划 ; SIS安全要求; SIS 的安全确认计划	SIS 的全部功能符合设计 ; SIS集成测试的结果 ; 安装、调试和确认活动的结果

表 F. 17给出了 SIS安装 、调试和确认的目的 、输入 、输出以及相关章节和条款的参考 。

F. 24 安装

SIS安装始于设计 、搭建设施 、过程设备 、动力源(例如 , 电力) 和仪表设备的可用性 ,止于 SIS从建造到运行的交接(即投运) 。该交接反映了通过运行进行的验收;此时进入调试(见 F. 24) 。

采购和实施收货检查功能的企业足以确保所规定的SIS设备以良好的工作状态被接收,并按GB/T 21109. 1— 2022的 11. 5 随附适当的文件以支持其使用。 临时贮存遵循各设备制造商的安全手册 ,并且包括对设备必要的预防性维护 。

请注意 ,需建立返修及重新安装的规程 , 以便实现对通过操作所发现的问题的纠正;该切换会造成相邻的设备处于不同的完工/验收状态(即安装和操作状态) 。对于这一项目来说 , 白色位号用来表示操作状态 ,绿色位号用来表示建造状态 。

每台仪器用它的仪表位号来识别 。SIS具有以下附加的可识别特性 :

- 所有的 SIS仪表都设有其作为 SIS设备的状态的可视化标识(即涂成红色) ;
- SIS机柜设有参考 SIS图号的铭牌;
- 将 SISHMI识别为(软件面板标识)SIS相关设备;
- 每台 SIF设备用显示其回路图的编号及 SIF编号的位号识别 。

建造不包括 AP的安装 。AP在设计过程中开发 、测试和验证 ,并且在试运行过程中引入到 SIS中 。

在投运前的建造验证活动包括 :

- 在接线中安装 “ringout” , 以确保正确接地和 SIS互连;
- 使包括 I/O在内的控制电路通电(从而确保没有短路或过载) ;
- “碰撞” (例如 ,激活短促的 “轻碰”)每台电机和每个阀门 , 以确保在正确的方向中运行;
- 确保所有的动力源(例如 ,气动装置)都是起作用的;
- 进行 “走查” ,验证安装的完整性 、安全性和正确性;
- 提供完整的 SIS竣工文件 。

使运行组参与到上述验证活动中 ,从而使运行组 :

- 了解 SIS设备的界区和位置;
- 了解动力源及其关键设备的位置[例如 ,断开 、过载和短路保护(如保险丝 、断路器)] ;
- 可以为其调试计划提供必要的细节(见 F. 25) ;
- 通过在建造的监督下实施此处讨论的所选的 SIS验证活动工作(例如 ， “ringout” SIS) ,维护组熟悉 SIS的安装 。

所完成的安装由包括建造 、运行和设计人员在内的检验小组来验证和审批 。完成时 ,将设备贴上位号 ，以反映运行的验收情况和所有权(即谁对该设备负责) 。

F. 25 调试

调试这一术语针对始于完成投运(即从建造到运行) 、止于验证SIS调试完成并能进行确认(见 F. 27)的时间段 。本例中 ,SIS的调试在 BPCS调试完成后立即开始 。

SIS调试包括对 SIS硬件系统校验和操作系统(即嵌入式软件) 校验的识别 、时间安排 、计划 、组织 、监督和文件编制 。

本例中 SIS的调试也称为 “校验” ，因为这一用语更好地反映了调试中实施的主要活动 。校验是 一项逐步推进的程序 ,它确保 :

- 所有的 SIS连通性都是正确的(包括接地) ;
- 所有的动力源(例如 ，电力 、气动装置)都能正确运行;
- 所有的 SIS设备(例如 ,传感器 、逻辑解算器 、最终元件 、HMI、工程师站 、通信系统) 均已通电并能正确运行;
- 传感器设置是正确的 。

在该阶段对使用固定编程语言(FPL) 的设备(例如 ,智能变送器) 进行检查 。在校验过 程 中 ，采 用 PE逻辑解算器工程师站及其 “强制” 功能 。 工厂维护组是该活动的重要组成部分 ,并根据需要由建造组和设计组提供支持 。在继续进行确认之前 ，由运行组批准试运行已完成并令人满意 。

F. 26 文档

宜有必要的文档供人员使用 。 因此 ,在继续进行确认之前 ,宜进行检查 ，以确保所有的文档都是可用且正确的 。

认可文件的最终清单包括 :

- H&RA文件[假设分析(表 F. 4) 、HAZOP(表 F. 5)] ;
- 可容忍风险排名(表 F. 8) ;
- 保护层的风险分配文档— 确定每个 SIF的 SIL(LOPA) ;
- 每个 SIF的测试规程(见 F. 27) ;

安全要求规范 ,包括 :

- P&I图 ;
- 逻辑图;
- AP打印纸版;
- 安全手册;
- 评估机构的安全性判定;
- 设备选择的判定方法文件;
- 制造商的安装说明;
- SIS硬件/AP/安装/维护文档;
- 系统性能力判定;
- SIF的 SIL验证计算(即 PFD_{avg}) ,包括气泡图 。

F. 27　确认

确认这一术语针对始于调试完成 、止于得出 SIS满足 SRS中定义的功能要求的结论的时间段 。

SIS的 确认从已经完成了 SIS的调试并完成 BPCS确认之后开始 。

SIS确认涉及对若干活动的识别 、时间安排 、计划 、组织 、监督和文件编制 。这些活动包括 :

- SIS硬件系统试车;
- SIS操作系统(即嵌入式软件)试车;
- SISAP试车;
- SIS启动(验收测试审批以及投产 ，即操作的分界) 。

本例 SIS的确认细分为 “试车” 和 “启动” ，以便更好地反映确认过程中实施的主要活动 。

试车是一项逐步进行的程序 ,在像制造成品一样运行过程时 ,通过使用非危险过程材料(例如 ,用水代替危险液体) ，以确保 SIS能正确地起作用 。为此 ,安装(见 F. 23)SIS逻辑解算器 AP,并对其所有操作模式(例如 ,启动 、运行 、停止)进行完善地测试(见 F. 27) 。生产人员是该阶段关键的参与者 ,并由维护组和设计组提供支持 。顺利完成试车并且由运行组批准后 ,将 SIS启动投产 。

启动是一项要求运行以预先批准的生产率安全地生产出高质量产品的活动 。在这 一 过程中 ,宜检查 SIS设备 ，以确保它们能正确工作 ,并能按试车过程执行其安全功能 。在该阶段完成后 ,记录结果 ,并由运行组完成最终审批 。SIS项目的确认即完成 。

F. 28　测试

F. 28讨论的多项所要求的测试均在SIS最初的确认过程中完成。 下文所述的测试规程也用于F. 29步骤 6 中所述的定期测试和检验 。

测试规程由 SIS的设计者编写 。该规程包括对由于 SIF测试造成安全事件的可能性的识别 。 因此 ,测试规程清楚地说明了如何安全地进行测试以及所需设备和人员的数量/质量 。

测试过程中包括以下活动 :

- 设备测试;
- 车间检测和校准;
- 仿真;
- 单独进行的逻辑测试;
- 自动测试;
- 手动测试;
- “调整前” 和 “调整后” 条件的文件编制;
- 详细说明每一 步的程序 。

有一些关键特性需要在刚好超过跳闸设定范围和最终控制设备的值进行测试 。需测试诊断程序(如失去信号)是会生成报警还是会将该过程带到安全状态 。需对 SIF锁存和复位逻辑进行测试 ,包括复位时最终控制设备的位置 。需将复位位置记录在文件中 ,并进行测试 。

宜测试 SIS与 BPCS的交互 。测试发送给 BPCS的 SIF指示 ,并测试根据这些指示所采取的任何动作 。单独测试 “镜像” SIS逻辑的 BPCS, 以证明两个系统均根据设计要求运行 。

SIF测试的通用规程如下 。

— 旁路其他 SIF, 以便测试目标 SIF。

—模拟正常操作条件 :

- 模拟正常操作条件中的仪表信号;
- 将目标最终控制设备置于正常的操作位置中;
- 将控制器和其他设备置于正常操作模式中 。

— 测试 SIF:

- 记录 SIF的实际跳闸点;
- 验证 SIF报警和最终控制设备上的动作;
- 验证 BPCS的 SIF相关动作 。

— 清除 SIF条件 :

- 验证处于安全状态时的 SIF动作 。

— 重置 SIF:

- 验证 SIF复位至设计状态的动作 。

该例的规程假设仪表已经经过了车间检测和校准 。该例的规程为 一 次性测试所有 SIS功能而编写 ,而不是每个 SIF各自的测试规程 。该规程首先检查主要的 SIS功能和最终控制设备 。 以下所列的每个测试动作均在无需重新测试最终控制设备的情况下对 SIF进行检测 。每个测试动作均给出了一个测试规程 ,以防变送器被更换或者跳闸设置被更改 。

顺利完成确认测试阶段的一个关键点是工厂操作和维护人员的参与情况 ,以保证他们清楚地了解过程 、BPCS和 SIS所有方面的情况 。这些人员包括 :

- 合格的控制室操作人员;
- 合格的电气和仪表技术人员 。

表 F. 18给出了仪表类型一览表以及所使用的一些测试规程 。

表 F. 18 仪表类型及所使用的测试规程一览表

压力	
正常连接	在主截止阀下游提供排放/通风口以及测试压力连接点
远程隔膜密封	宜为在线测试提供隔离阀和校准环。 在确认校准的过程中,考虑相对于管嘴的高度以及毛细管充装液体的比重
温度	
热电偶	可以对设备执行连续性检查 ,以便仅确定可操作性 。根据标准曲线 ,在已知温度下验证毫伏输出
电阻温度检测器(RTD)	可测定电阻 ,以验证设备的可操作性 。根据电阻的标准校准表 ,在已知温度下验证阻值
充填式系统	取下传感装置 ,并放在温度浴槽中
双金属温度开关	取下传感装置 ,并放在温度浴槽中

以下规程是确认 SIS功能(包括诊断报警)的示例 。该示例不包括对 BPCS功能的测试 。每个 SIS设备(例如 ,传感器 、逻辑解算器 、最终元件)均有制造商推荐的测试 。这些测试(或替换) 在本例规程中可能不涉及 ,但假定会单独实施 。参考 ISA TR 84. 00. 03:2012《安全仪表系统(SIS)的机械完整性》。关于测试规程的示例 ,请参考制造商的安全手册中检验测试章节 。完整的测试规程可能还包括以下方面的测试 :

- 安全功能被激活时 BPCS的动作 ,如控制器切换至手动模式;
- BPCS “镜像” 联锁功能;
- BPCS对安全系统诊断的报警;
- 作为 LOPA 中分配的安全层的 BPCS报警 。

下文给出了反应器 R1联锁检查规程的示例 。

以下规程中引用了 NOMEX。

标题：	反应器 R1 联锁检查规程	编制：		日期：
		修订：		日期：
区域：		技术审核：	____	日期：
PSM 关键：	是	最终批准：	____	日期：

□存档原件　　□现场副本

测试总结

A. 被测传感器/开关

位号	零点	量程	正常值	正常值	报警值	报警值	跳闸值	跳闸值	容许偏差
100PT	0	1. 378MPa	0. 689MPa	1 2 mA	0. 7924 MPa	13. 2 mA	0. 8613 MPa	14mA	±0. 01378MPa
100PT1	0	1. 378MPa	0. 689MPa	1 2 mA	0. 7924 MPa	13. 2 mA	0. 8613 MPa	14mA	±0. 0137 MPa
100TT	0	121 ℃	51 ℃	1 2 mA	82 ℃	15. 52mA	93 ℃	16. 8 mA	±16. 7 ℃
200PT	0	0. 1378 MPa	0. 0172 MPa	6 mA	0. 0345 MPa	8 mA	0. 0689 MPa	1 2 mA	±0. 00689MPa

B. 被测最终控制设备

位号	位置
100PV	打开
100PV1	打开

C. 测试结果：

检查一：

_____所有的设备均通过测试 。

_____需校正动作以通过测试 。

完成检查程序的 日期：_____。

D. 安全 & 健康

- 按区域规程所要求的个人防护设备(例如安全眼镜 、安全帽 、安全鞋) 。

E. 特殊防护设备

- 根据需要将 NOMEX用于闪光保护 。

F. 预测试条件和锁定

- 反应器需清空物料并锁定 ,采用上锁挂牌(LOTO)规程 ；
- 宜不激活紧急停车系统 ；
- 宜根据需要在适当的位置设置屏障 ；
- 沟通(例如签字 、备忘录 、时间安排 、计划)宜完整完成 。

G. 许可

- 每台变送器按线的断路许可 。

H. 特殊设备

- 一 台电流信号发生器 ；
- 一 台变送器手操器 。

I. 参考纸版文件

- P&ID# ；

- 逻辑图页#；
- 电仪图#。

J. 人力资源

- 合格的控制室操作员;
- 合格的电气和仪表技术人员。

每个联锁测试规程均有自己独特的安全考虑。为了满足特定的应用要求,宜对以下正文进行修改。

校准和检验

A. 已校准或已验证校准仪表：

按维护规程校准仪表。

位号	描述	跳闸值	校验前	初始值	日期
100PT	北侧反应器的压力				
100PT1	南侧反应器的压力				
100TT	反应器温度				
200PT	反应器密封圈压力				

B. 已检验的仪表和最终控制设备：

已检验了接线、管路、过滤器、就地表头、电磁阀、保温层和工艺过程连接等的现场安装问题。

位号	描述	检验前	检验后	初始值	日期
100PT	反应器北侧的压力				
100PT1	反应器南侧的压力				
100TT	反应器温度				
200PT	反应器密封压力				
100PV	反应器北侧的排放阀				
100PV1	反应器南侧的排放阀				

联锁测试规程

检查规程起始时间：_____日期：_____

执行规程的经手人：

头衔	签名	日期
控制室操作员		
电仪技术人员		
电仪技术人员		
操作主管		

联锁检查规程的一般设置

电仪技术人员：

A. 模拟正常操作条件。

_____解除 100PV 和 100PV1上的所有 BPCS联锁。

_____更新旁路 #1 的旁路检查表。

反应器 SIS停车按钮的联锁检查规程

测试频次：	6个月
测试目标：	反应器安全系统手动停车,需打开反应器压力控制阀 100PV 和 100PV1。此外,测试最终控制设备的诊断

A. 解除联锁 。 (控制室操作员)

_____通过按下复位按钮 PB000,复位反应器安全系统 。
_____验证反应器安全系统的激活指示灯 EA010被点亮 。
_____验证反应器安全系统的非激活指示灯 EA011未点亮 。

B. 模拟正常条件 。 (控制室操作员)

_____验证反应器排放阀关闭诊断报警 EA18未点亮 。
_____根据 BPCS,关闭反应器排放阀 100PV。
_____根据 BPCS,关闭反应器排放阀 100PV1。
_____将所有的 BPCS控制器设置到正常操作位置 。
_____将所有的 BPCS控制器设置到正常操作模式 。
_____将所有的 BPCS阀门和电机设置到正常模式 。

C. 现场验证正常条件 。 (现场操作员)

_____现场验证反应器排放阀 100PV 已关闭 。
_____现场验证反应器排放阀 100PV1已关闭 。

D. 测试诊断报警 。 (电仪技术人员)

_____断开来自反应器排放阀关闭限位开关 100LSC的信号 。
_____验证反应器排放阀关闭诊断报警 EA18被点亮 。
_____重新连接来自反应器排放阀关闭限位开关 100LSC的信号 。
_____验证反应器排放阀关闭诊断报警 EA18未点亮 。
_____断开来自反应器排放阀关闭限位开关 100LSC1的信号 。
_____验证反应器排放阀关闭诊断报警 EA18被点亮 。
_____重新连接来自反应器排放阀关闭限位开关 100LSC1的信号 。
_____验证反应器排放阀关闭诊断报警 EA18未点亮 。

E. 测试联锁 。 (控制室操作员)

_____通过按下停车按钮 500PB,关闭反应器安全系统 。

F. 验证联锁动作 。 (控制室操作员)

_____验证反应器安全系统激活指示灯 EA0101未点亮 。
_____验证反应器安全系统非激活指示灯 EA011被点亮 。
_____验证反应器排放阀打开诊断报警 EA17未点亮 。
_____从 BPCS,验证反应器排放阀 100PV被打开 。
_____从 BPCS,验证反应器排放阀 100PV1被打开 。
_____验证所有的 BPCS控制器被设置到安全位置 。
_____验证所有的 BPCS控制器被设置到安全模式 。
_____验证所有的 BPCS阀门和电机处于安全模式中 。

G. 现场验证正常条件 。 (现场操作员)

_____现场验证反应器排放阀 100PV被打开 。
_____现场验证反应器排放阀 100PV1被打开 。

H. 测试诊断报警 。 (电仪技术人员)

_____断开来自反应器排放阀关闭限位开关 100LSO 的信号 。

_____验证反应器排放阀打开诊断报警 EA17被点亮 。

_____重新连接来自反应器排放阀关闭限位开关 100LSO 的信号 。

_____验证反应器排放阀打开诊断报警 EA17未点亮 。

_____断开来自反应器排放阀关闭限位开关 100LSO1的信号 。

_____验证反应器排放阀打开诊断报警 EA17被点亮 。

_____重新连接来自反应器排放阀打开限位开关 100LSO1的信号 。

_____验证反应器排放阀打开诊断报警 EA17未点亮 。

I. 解除联锁 。 (控制室操作员)

_____通过按下复位按钮 PB000,复位反应器安全系统 。

_____验证反应器安全系统的激活指示灯 EA010被点亮 。

_____验证反应器安全系统的非激活指示灯 EA011未点亮 。

_____验证反应器排放阀打开诊断报警 EA17未点亮 。

J. 现场验证复位条件 。 (现场操作员)

_____现场验证反应器排放阀 100PV被打开 。

_____现场验证反应器排放阀 100PV1被打开 。

K. 验证复位条件 。 (控制室操作员)

_____从 BPCS,验证反应器排放阀 100PV被打开 。

_____从 BPCS,验证反应器排放阀 100PV1被打开 。

_____验证所有的 BPCS控制器被设置到安全位置 。

_____验证所有的 BPCS控制器被设置到安全模式 。

_____验证所有的 BPCS阀门和电机处于安全模式中 。

反应器压力 100PT联锁检查规程

SIF	S1、S2
事件名称：	反应器的过压
事件分类：	SIL2
测试频次：	6个月
测试目标：	反应器的压力高时 ,打开反应器的压力控制阀 100PV和 100PV1

A. 运行诊断(电仪技术人员)

_____将手操器连接至反应器压力变送器 100PT并运行变送器诊断 。

_____验证没有诊断错误 。

B. 模拟正常条件 。 (控制室操作员)

_____通过按下复位按钮 PB000,复位反应器安全系统 。

_____验证反应器安全系统激活指示灯 EA010被点亮 。

C. 测试联锁 。 (电仪技术人员)

_____从安全系统中断开反应器压力变送器 100PT。

D. 验证联锁动作 。 (控制室操作员)

_____验证反应器安全系统非激活指示灯 EA011被点亮 。

_____验证反应器安全系统变送器诊断报警 EA014被点亮 。

_____验证在按下复位按钮 PB000时 ,反应器安全系统将不复位 。

E. 模拟正常条件 。 (电仪技术人员)

_____将信号发生器连接至反应器压力变送器 100PT。

_____在反应器压力变送器 100PT 中模拟 0. 689MPa(12mA) 。
_____更新旁路 #2 的旁路检查表 。

F. 模拟正常条件 。 (控制室操作员)

_____验证反应器安全系统变送器诊断报警 EA014未点亮 。
_____按下复位按钮 PB000,复位反应器安全系统 。
_____验证反应器安全系统激活指示灯 EA010被点亮 。

G. 测试联锁 。 (电仪技术人员)

_____将反应器压力变送器 100PT 中的模拟信号缓慢提高至 0. 8613 MPa(14mA) 。
_____记录联锁跳闸时的设置 :_____。

H. 验证联锁动作 。 (控制室操作员)

_____验证反应器安全系统非激活指示灯 EA011被点亮 。
_____验证反应器安全系统变送器跳闸报警 EA012被点亮 。
_____验证在按下复位按钮 PB000时 ,反应器安全系统将不复位 。

I. 解除联锁 。 (电仪技术人员)

_____将反应器压力变送器 100PT 中的模拟信号缓慢降低至 0. 689MPa(12mA) 。

J. 验证复位条件 。 (控制室操作员)

_____按下复位按钮 PB000,复位反应器安全系统 。
_____验证反应器安全系统的激活指示灯 EA010被点亮 。
_____验证反应器安全系统变送器的跳闸报警 EA012未点亮 。

K. 返回至当前状态 。 (电仪技术人员)

_____从反应器压力变送器 100PT 中断开信号发生器 。
_____将反应器压力变送器 100PT重新连接至安全系统 。
_____更新旁路 #2 的旁路检查表 。

L. 验证当前状态 。 (控制室操作员)

_____验证反应器压力变送器 100PT可读取实际的反应器压力 。

反应器压力 100PT1联锁检查规程

SIF	S2
事件名称 :	反应器的过压
事件分类 :	SIL2
测试频次 :	6个月
测试目标 :	反应器的压力高时 ,打开反应器的压力控制阀 100PV和 100PV1

A. 运行诊断 。 (电仪技术人员)

_____将手操器连接至反应器压力变送器 100PT1并运行变送器诊断 。
_____验证没有诊断错误 。

B. 模拟正常条件 。 (控制室操作员)

_____按下复位按钮 PB000,复位反应器安全系统 。
_____验证反应器安全系统激活指示灯 EA010被点亮 。

C. 测试联锁 。 (电仪技术人员)

_____从安全系统中断开反应器压力变送器 100PT1。

D. 验证联锁动作 。 (控制室操作人员)

_____验证反应器安全系统非激活指示灯 EA011被点亮 。

_____验证反应器安全系统变送器诊断报警 EA014被点亮 。

_____验证在按下复位按钮 PB000时 ,反应器安全系统将不复位 。

E. 模拟正常条件 。 (电仪技术人员)

_____将信号发生器连接至反应器压力变送器 100PT1。

_____在反应器压力变送器 100PT1中模拟 0. 689MPa(12mA) 。

_____更新旁路 #3 的旁路检查表 。

F. 模拟正常条件 。 (控制室操作员)

_____验证反应器安全系统变送器诊断报警 EA014未点亮 。

_____按下复位按钮 PB000,复位反应器安全系统 。

_____验证反应器安全系统激活指示灯 EA010被点亮 。

G. 测试联锁 。 (电仪技术人员)

_____将反应器压力变送器 100PT1中的模拟信号缓慢提高至 0. 8613 MPa(14mA) 。

_____记录联锁跳闸时的设置 :_____。

H. 验证联锁动作 。 (控制室操作员)

_____验证反应器安全系统非激活指示灯 EA011被点亮 。

_____验证反应器安全系统变送器跳闸报警 EA012被点亮 。

_____验证在按下复位按钮 PB000时 ,反应器安全系统将不复位 。

F. 解除联锁 。 (电仪技术人员)

_____将反应器压力变送器 100PT1中的模拟信号缓慢降低至 0. 689MPa(12mA) 。

J. 验证复位条件 。 (控制室操作员)

_____按下复位按钮 PB000,复位反应器安全系统 。

_____验证反应器安全系统的激活指示灯 EA010被点亮 。

_____验证反应器安全系统变送器的跳闸报警 EA012未点亮 。

K. 返回至当前状态 。 (电仪技术人员)

_____从反应器压力变送器 100PT1中断开信号发生器 。

_____将反应器压力变送器 100PT1重新连接至安全系统 。

_____更新旁路 #3 的旁路检查表 。

L. 验证当前状态 。 (控制室操作员)

_____验证反应器压力变送器 100PT1可读取实际的反应器压力 。

反应器温度 100TT联锁检查规程

SIF	S1
事件名称 :	反应器的温度过高
事件分类 :	SIL2
测试频次 :	6个月
测试目标 :	反应器的温度高时 ,打开反应器的压力控制阀 100PV和 100PV1

A. 运行诊断 。 (电仪技术人员)

_____将手操器连接至反应器温度变送器 100TT并运行变送器诊断 。

_____验证没有诊断错误 。

B. 模拟正常条件 。 (控制室操作员)

_____按下复位按钮 PB000,复位反应器安全系统 。

_____验证反应器安全系统激活指示灯 EA010被点亮 。

C. 测试联锁 。 (电仪技术人员)

_____从安全系统中断开反应器温度变送器 100TT。

D. 验证联锁动作 。 (控制室操作员)

_____验证反应器安全系统非激活指示灯 EA011被点亮 。

_____验证反应器安全系统变送器诊断报警 EA014被点亮 。

_____验证在按下复位按钮 PB000时 ,反应器安全系统将不复位 。

E. 模拟正常条件 。 (电仪技术人员)

_____将信号发生器连接至反应器温度变送器 100TT。

_____在反应器温度变送器 100TT 中模拟 51. 7 ℃(12mA) 。

_____更新旁路 #4 的旁路检查表 。

F. 模拟正常条件 。 (控制室操作员)

_____验证反应器安全系统变送器诊断报警 EA014未点亮 。

_____按下复位按钮 PB000,复位反应器安全系统 。

_____验证反应器安全系统激活指示灯 EA010被点亮 。

G. 测试联锁 。 (电仪技术人员)

_____将反应器温度变送器 100TT 中的模拟信号缓慢提高至 93. 3 ℃(16. 8 mA) 。

_____记录联锁跳闸时的设置 :_____。

H. 验证联锁动作 。 (控制室操作员)

_____验证反应器安全系统非激活指示灯 EA011被点亮 。

_____验证反应器安全系统变送器跳闸报警 EA012被点亮 。

_____验证在按下复位按钮 PB000时 ,反应器安全系统将不复位 。

I. 解除联锁 。 (电仪技术人员)

_____将反应器温度变送器 100TT 中的模拟信号缓慢降低至 51. 7 ℃(12mA) 。

J. 验证复位条件 。 (控制室操作人员)

_____按下复位按钮 PB000,复位反应器安全系统 。

_____验证反应器安全系统的激活指示灯 EA010被点亮 。

_____验证反应器安全系统变送器的跳闸报警 EA012未点亮 。

K. 返回至当前状态 。 (电仪技术人员)

_____从反应器温度变送器 100TT 中断开信号发生器 。

_____将反应器温度变送器 100TT重新连接至安全系统 。

_____更新旁路 #4 的旁路检查表 。

L. 验证当前状态 。 (控制室操作员)

_____验证反应器温度变送器 100TT可读取实际的反应器温度 。

反应器密封压力 200PT 的联锁检查程序

SIF	S3
事件名称 :	反应器密封的过压
事件分类 :	SIL2
测试频次 :	6个月
测试目标 :	反应器密封的压力高时 ,打开反应器的压力控制阀 100PV和 100PV1

A. 运行诊断 。 (电仪技术人员)

_____将手操器连接至反应器压力变送器 200PT并运行变送器诊断 。

_____验证没有诊断错误 。

B. 模拟正常条件 。 (控制室操作员)

_____按下复位按钮 PB000,复位反应器安全系统 。

_____验证反应器安全系统激活指示灯 EA010被点亮 。

C. 测试联锁 。 (电仪技术人员)

_____从安全系统中断开反应器压力变送器 200PT。

D. 验证联锁动作 。 (控制室操作员)

_____验证反应器安全系统非激活指示灯 EA011被点亮 。

_____验证反应器安全系统变送器诊断报警 EA014被点亮 。

_____验证在按下复位按钮 PB000时 ,反应器安全系统将不复位 。

E. 模拟正常条件 。 (电仪技术人员)

_____将信号发生器连接至反应器密封压力变送器 200PT。

_____在反应器密封压力变送器 200PT 中模拟 0. 017MPa(6mA) 。

_____更新旁路 #5 的旁路检查表 。

F. 模拟正常条件 。 (控制室操作员)

_____验证反应器安全系统变送器诊断报警 EA014未点亮 。

_____按下复位按钮 PB000,复位反应器安全系统 。

_____验证反应器安全系统激活指示灯 EA010被点亮 。

G. 测试联锁 。 (电仪技术人员)

_____将反应器密封压力变送器 200PT 中的模拟信号缓慢提高至 0. 0689 MPa(12mA) 。

_____记录联锁跳闸时的设置:_____。

H. 验证联锁动作 。 (控制室操作员)

_____验证反应器安全系统非激活指示灯 EA011被点亮 。

_____验证反应器安全系统变送器跳闸报警 EA012被点亮 。

_____验证在按下复位按钮 PB000时 ,反应器安全系统将不复位 。

I. 解除联锁 。 (电仪技术人员)

_____将反应器密封圈压力变送器 200PT 中的模拟信号缓慢降低至 0. 0172 MPa(6mA) 。

J. 验证复位条件 。 (控制室操作员)

_____按下复位按钮 PB000,复位反应器安全系统 。

_____验证反应器安全系统的激活指示灯 EA010被点亮 。

_____验证反应器安全系统变送器的跳闸报警 EA012未点亮 。

K. 返回至当前状态 。 (电仪技术人员)

_____从反应器密封压力变送器 200PT 中断开信号发生器 。

_____将反应器压力变送器 200PT重新连接至安全系统 。

_____更新旁路 #5 的旁路检查表 。

L. 验证当前状态 。 (控制室操作员)

_____验证反应器密封压力变送器 200PT可读取实际的反应器温度 。

联锁检查规程的总体完成情况

电仪技术人员:

A. 将所有其他联锁返回至运行状态 。

_____将 100PV 和 100PV1上所有的 BPCS联锁返回至投用状态 。

_____更新旁路 #1 的旁路检查表 。

测试和检验由以下人员完成:

头衔	签名	日期
控制室操作员		
控制室操作员		
电仪技术人员		
电仪技术人员		
操作主管		

完成检查规程的时间：_____日期：_____

测试后的检验和文件编制

A. 验证对规程所做的任何更改都已经过管理层的复审和批准 。

B. 如果检出设备失效，需要采取什么纠正动作：

_____

_____

_____

_____

_____

完成在存档原件和安全系统测试记录文件上的签字 。表 F. 19给出了针对联锁检查规程的旁路/模拟如何形成书面检查表的示例 。

表 F. 19 联锁检查规程旁路/模拟检查表

旁路 #	回路	位置	方法	设置步骤	初始值	解除步骤	初始值
1	DCS	DCS	标志	1. 1		7. 1	
2	100PT	变送器	信号发生器	3. 4		3. 10	
3	100PT1	变送器	信号发生器	4. 4		4. 10	
4	100TT	变送器	信号发生器	5. 4		5. 10	
5	200PT	变送器	信号发生器	6. 4		6. 10	
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

F. 29　步骤 F.6:SIS操作和维护

表 F. 20　SIS安全生命周期— 方框 6

概述					
安全生命周期阶段或活动		目标	GB/T 21109. 1— 2022 的要求章节或小节	输入	输出
GB/T 21109. 1— 2022 的图 7, 方框 6	SIS 运行和维护	确保在操作和维护期间保持 SIS 的功能安全	16	SIS安全要求； SIS设计； SIS的操作和维护计划	操作和维护活动的结果

在系统投入运行之前，宜对运行 、维护和其他支持人员进行关于 BPCS和 SIS二者功能的培训，并在对系统做出任何更改时，随时更新培训 。

关于 SIS的操作和维护培训，需要考虑的新项目包括：

- 术语(例如，SIS、SIF、PFD_{avg}、SIL、保护层)；
- 危险和风险分析；
- 架构[例如，HMI(SIS和 BPCS) 、SIS接口(例如来自 BPCS的只读链路)]；
- 文件编制要求(例如，对 SIF/SIS的要求频率 、规程/方法/技术 、检验测试和检验 、测试结果 、细化到修订版次级别的设备标识位号 、负责人员/部门/组织)；
- 旁路规程；
- SIF/SIS的测试频次；
- SIS的功能描述 。

为操作和维护制定 SIS跳闸 日志，以记录 SIS的需求和失效 。见表 F. 21。

SIF的误跳闸也包含在此日志中，但不计入对 SIS的要求率统计 。

表 F. 21　SIS跳闸 日志

日期	SIF	要求/误跳闸	跳闸原因	事件报告 #	记录人
5/18/08	S-2	要求	操作员失误— 造成反应器过充	严重事件 报告 # 18	L. Soft
8/03/08	S-3	误跳闸	变送器 200PT失效	无	J. Doe
2/28/09	S-1	要求	冷却剂控制回路失效	严重事件 报告 # 43	T. Rex

使用跟踪系统识别 SIS设备在测试过程中检测到重复发生的问题 。如表 F. 22 的记录结果 。

表 F. 22　SIS设备失效日志

日期	设备	安全/危险失效	失效描述	记录人
3/21/07	100TT	安全	超校准范围	T. Rex
5/18/08	100PV	危险	阀杆被卡住— 不能打开	L. Soft

表 F. 22 SIS设备失效日志（续）

日期	设备	安全/危险失效	失效描述	记录人
8/03/08	100PV	危险	阀杆被卡住— 不能打开	J. Doe
2/28/09	100PV	危险	阀杆被卡住— 不能打开	T. Rex

如表 F. 22所示，排放阀 100PV经常出问题 。 出现第三次失效后，通过根因失效分析确定了阀门存在缺陷 。更换该阀门后，再未出现失效 。

始终维护 BPCS和 SIS中实现的当前控制和安全逻辑文件 。 在执行任何更改后，随时将更改记录在文件中 。对这些充分描述系统及其功能的文件的硬拷贝做维护，以供参考 。

实施审计程序，要求对系统文档作为周期性过程危险复审的一部分进行检查 。 出具报告，说明审计结果，并标记审计的建议以便进行跟踪(每季度进行一次)，直至完成 。审计包括：

- 复审自上一次复审以来所作的全部更改，验证文件状态是否正确；
- 复审自上次复审以来与 SIS有关的设备或逻辑涉及的所有问题，以确定潜在的问题是否会在将来使系统功能降级；
- 复审操作人员对系统功能和运行的认识；
- 复审 SIS要求日志，以确认 LOPA 中所用的要求率假设；
- 复审 SIF测试结果，以确认 PFD_{avg}计算中所用的设备失效率假设 。

以下为将包括在审计中的支持文件清单 。这些文件供操作人员使用，并保持最新 。

- H&RA文档[假设分析(表 F. 4)，HAZOP(表 F. 5)]；
- 所使用的可容许风险分级(即表 F. 8)
- 将风险分配给保护层的记录文件— 确定每个 SIF的 SIL(LOPA)(即表 F. 9)；
- P&I图(即图 F. 3 和图 F. 10)；
- SIF系统图(即图 F. 12)；
- AP打印件(梯形逻辑图)(即图 F. 11)；
- 安全手册；
- SIS硬件/AP/安装/维护文档(例如，表 F. 20— 方框 6)；
- 系统性能力文件；
- 每个 SIF的 SIL验证计算(即 PFD_{avg})，包括气泡图(即图 F. 4~图 F. 9)；
- 每个 SIF的测试规程；
- 对每个 SIF的过程要求(即表 F. 12)；
- SIF设备的失效数据(即表 F. 13) 。

按 PFD_{avg}计算中规定的频率(即每六个月)进行 SIS的定期测试和检验 。 同样以六个月的频率测试 LOPA 中识别出的保护层 。

操作部门要保持相关记录用于证实已经按要求完成了检验测试和检验 。这些记录宜至少包括以下信息：

a) 所执行测试和检验的描述；
b) 测试和检验日期；
c) 执行测试和检验的人员姓名；
d) 被测系统的序列号或其他唯一性标识(例如，回路号 、位号号 、设备号和 SIF号)；
e) 测试和检验的结果(例如，“校验前”和“校验后”的状态)；
f) 当前在 SIS逻辑解算器中的运行的 AP版本 。

F.30 步骤 F.7:SIS变更

表 F.23 SIS安全生命周期— 方框 7

概述					
安全生命周期阶段或活动		目标	GB/T 21109.1— 2022 的要求章节或小节	输入	输出
GB/T 21109. 1— 2022 的图 7, 方框 7	SIS变更	对 SIS 进行校正、增强或改造以确保达到和保持要求的 SIL	17	修改后的 SIS安全要求	SIS修改结果

表 F.23给出了 SIS变更的目的 、输入 、输出以及相关章节和小节的参考 。

工厂具备符合 OSHA 29CFR 1910.119的对变更过程的管理 。对 SIS进行任何变更时,要求重新进入 SIS安全生命周期的合适步骤 。

F.31 步骤 F.8:SIS停用

表 F.24中概括了关键设备的停用过程 。

表 F.24 SIS安全生命周期— 方框 8

概述					
安全生命周期阶段或活动		目标	GB/T 21109.1— 2022 的要求章节或小节	输入	输出
GB/T 21109. 1— 2022 的图 7, 方框 8	停用	确保适当的审查,获得授权,并确保 SIF 适当保留	18	竣工安全要求和过程信息	停用的 SIF

工厂具有停用危险过程方面的经验,并了解需要在停用计划以后进行 H&RA 和工程分析 。完成这些工作之后,在开始停用之前需获得适当的授权,并安排好时间 。

F.32 步骤 F.9:SIS验证

验证(表 F.25)是贯穿 SIS的整个生命周期中执行的一项活动 。

表 F.25 SIS安全生命周期— 方框 9

概述					
安全生命周期阶段或活动		目标	GB/T 21109.1— 2022 的要求章节或小节	输入	输出
GB/T 21109. 1— 2022 的图 7, 方框 9	SIS验证	测试和评估给定阶段的输出,以确保作为该阶段输入的产出和标准的正确性和一致性	7.12.5	每个阶段 SIS 的验证计划	每个阶段 SIS 验证的结果

工程 、运行和维护人员共同协调验证计划，以使各组织实现其目标 。

工程人员通过验证来确保：

- 工程的硬件 、AP和系统设计是正确的 ,并与 SRS一致；
- 操作人员从验证起始便参与到选定验证活动中(例如 AP开发 、HMI画面) ,这样最终的审批不会产生意料之外的结果(例如 ,大幅返工 、延误)；
- 维护员有处理 SIS设备/子系统/系统的实际操作机会，以便熟悉文档 、硬件位置 、AP功能，同时也便于验证 。

操作人员进行验证的目的是：

- 确定该项目按计划如期进行；
- 作为编写操作说明书的输入 。

维护人员进行验证的目的是：

- 使人员熟悉工艺过程；
- 识别需要哪些方面进行新培训/购置新的维护工具；
- 识别与工厂实践不一致的安装规程；
- 制定维护规程 。

F. 33 步骤 F. 10:功能安全管理和 SISFSA

表 F. 26 SIS安全生命周期— 方框 10

概述					
安全生命周期阶段或活动		目标	GB/T 21109. 1— 2022 的要求章节或小节	输入	输出
GB/T 21109. 1— 2022 的图 7, 方框 10	功能安全管理和 SISFSA	对 SIS所达到的功能安全进行调查并做出判断	5	SIS FSA 计划编制 SIS安全要求	SISFSA 结果

F. 34 功能安全管理

F. 34. 1 概述

本公司的功能安全管理(表 F. 26) 根据过程安全管理(PSM) 程序实现。 有广泛的企业标准针对 PSM 的各个方面 ,如机械完整性 、质量保证和培训 。 这些标准要求 ,在适用时 ,所有在公司生产设施实施的新项目需符合 IEC 61511 的要求 。

F. 34. 2 人员能力

为了确保负责执行和复审每项 SIS安全生命周期活动的人员具有执行其所负责活动的能力 ,需要进行管理 。这可以通过实施 GB/T 21109. 1— 2022的 12. 5. 2 中概括的方法来实现 。所复审的资格认定内容为：

- 经验和培训；
- 工艺过程的工程知识；
- SIS技术的工程知识；
- 安全工程知识(例如企业的功能安全标准)；
- 管理和领导技能；

- 对事件潜在后果的了解 。

此外 ,对于操作和维护人员 ,需要针对与工艺过程相关的危险进行培训 ,并在 BPCS和 SIS启动之前 ,进行其操作培训 。

F. 35　功能安全评估

在过程启动之前,宜执行FSA(也称为启动前的安全复审);见GB/T 21109. 1— 2022的5. 2. 6. 1。FSA 的总体目的是 ,确保 SIS将根据 SRS规定的要求运行 ,这样 SIS才能安全地从安装阶段进入到生产阶段 。

在完成和批准所有的验证活动之后 ,方可执行 FSA。

附 录 G
（资料性）
应用程序开发实践的指南

G. 1 目的

在过程工业领域中，PE设备的选择(见 GB/T 21109. 1— 2022的 11. 5 和 11. 6)或者基于有安全手册支持的，符合 IEC 61508-3 的设备(例如，安全 PLC)，或选择基于以往使用 。

本附录 G提供了被称为“通用安全应用编程属性”的注意事项示例，这些注意事项需以合适的方式，在制造商提供的安全手册或项目特定编程手册中加以说明，用以保持 AP设计在 GB/T 21109范围内，并有助于实现 AP预期的安全系统性完整性 。

注：本附录之前为 GB/T 21109. 2— 2007的附录 A。

G. 2 一般安全应用编程属性

本附录描述了安全应用编程的通用属性或与语言无关的属性 。这些属性是在一个分层的三层框架中定义的 。 四个顶级属性包括：

可靠性：可靠性是指 AP在设计依据中规定的条件下的可预测和 一 致的性能 。 这个顶级属性对于安全性很重要，因为它降低了在实现过程中会被引入到 AP中从而造成不成功运行的故障的可能性 。

鲁棒性：鲁棒性是 AP以可接受的方式在异常过程条件或事件下运行的能力 。 这 一 顶级属性对于安全性来说是很重要的，因为它提高了 AP处理异常条件 、从内部失效中恢复 、防止由于异常情况(并非所有的情况已经在设计基础上进行了充分定义)引起的错误传播的能力 。

可追溯性：可追溯性与审查和识别 AP、库装置起源 、开发过程的可行性有关，即交付的 AP可以显示为严格实施过程的产物 。可追溯性还包括能够将 AP与更高级别的设计文档相关联 。这个顶级属性对安全性很重要，因为它有助于进行验证和确认，以及 AP质量保证的其他方面 。

可维护性：AP降低在调试后所做更改期间引入故障的可能性的方法 。 这个顶级属性对安全性很重要，因为它降低了 自适应 、纠正或完善 AP维护期间由故障导致操作失败的可能性 。

G. 3 可靠性

G. 3. 1 概述

在 AP编程的语境中，可靠性是(1)在定义的时间间隔内和定义的条件下成功执行的可能性，或者(2)按需成功操作的可能性 。AP执行到完成是其关于系统内存和 AP逻辑的正确行为的结果 。AP是否产生及时的输出取决于自动化工程师对语言结构和运行时环境特性的理解 。 因此，所述可靠性的中间属性是：

- 内存使用的可预测性：AP具备较高的可能性使其不会造成逻辑解算器访问非预期的或非允许的内存;
- 控制流的可预测性：逻辑解算器具备极高的可能性使其按照程序员的设计意图按顺序执行指令;
- 时间特性的可预测性：AP具备极高的可能性使其在定义的运行时环境中执行时满足响应时间和容量的约束;数学或逻辑结果的可预测性：AP具备极高的可能性使其在定义的运行时环境中产生自动化工程师预期的数学或逻辑(运算)的结果 。

G. 3. 2　内存使用的可预测性

G. 3. 2. 1　尽可能减少动态内存分配

动态内存分配在 AP中用于在程序运行时，根据需要临时获取(分配)内存，并在不再需要时释放内存(也包括在程序运行时)用于其他用途 。安全问题是，当在实时系统中动态分配内存时，AP随后可能不会释放全部或部分内存 。这可能是因为：

- AP将内存分配给自己，但不会将其作为正常执行路径的一部分释放，或
- 在执行释放内存的语句之前，临时分配内存给自身的 AP在执行过程中被中断 。

这两种情况中的任何一种都将导致所有可用内存的最终丢失和所有安全系统功能的丧失 。 因此，宜尽量减少数字安全系统中的动态内存分配 。

如果动态内存分配不可避免，则 IEC 61508-3适用，且 AP需包括以下规定，以确保：

- 在特定执行周期内动态分配的全部内存均在该周期结束时被释放;
- 将在动态分配内存点和释放内存点之间执行中断的可能性最小化(如果不能完全避免);AP中还需有检测动态分配的内存没有被释放的情况的规定，并释放这样的内存 。

因此，IEC 61511不鼓励使用间接寻址 。IEC 61508-3适用于使用间接寻址的 AP。

G. 3. 2. 2　最小化内存分页和交换

内存分页是在主存储区域中使用一部分内存来存储不经常使用的信息 。 当运行中的 AP需要这些存储区时，逻辑解算器将它们从内存的一部分读取并加载回内存的另 一 部分 。进程交换是使用部分内存来存储整个非运行进程(包括其数据区域，如堆栈空间和堆空间)的内存映像 。

当要执行进程时，镜像从存储器的一部分加载回主存储器，供逻辑解算器使用 。在任何情况下，用于交换的内存和存储部分的具体使用情况都是不确定的 。

这些功能不适用于安全系统，因为这些内存和存储使用的不确定性反过来会导致响应时间的显著延迟，以及使用复杂的中断驱动功能来处理内存传输 。

如果 SIS中使用了支持内存分页或进程交换的逻辑解算器，则需在逻辑解算器层级禁用此功能 。需为所有数据和 AP提供足够的主内存 。如果对这些功能未被禁用有任何疑问，则 IEC 61508-3 适用，并且 AP中应规定确保所有关键功能及其数据区域在整个执行期间都在主存储器中 。AP 中的这些规定包括逻辑解算器调用(“固定 pinning”)、应用编程工具指令和逻辑解算器脚本 。

G. 3. 3　控制流的可预测性

G. 3. 3. 1　概述

控制流定义 AP中语句的执行顺序 。可预测的控制流允许对程序在指定条件下的执行方式进行明确的评估 。

相关的基本属性为：

- 结构最大化;
- 控制流复杂性的最小化;
- 使用前初始化变量;
- 子程序的单一入口和出口点;
- 最小化接口歧义;
- 使用数据类型;
- 考虑准确度和精度;
- 算术 、逻辑和函数运算符的优先顺序;

- 避免有副作用的功能或程序;
- 将赋值与求值分开;
- 正确处理程序插装;
- 控制类库的大小;
- 尽量减少动态绑定的使用;
- 控制运算符重载 。

G. 3. 3. 2 最大化结构

需避免带有 GOTO或等效执行控制语句的 AP,这些语句会导致 AP 的执行从 一 个分支非结构化地转移到另一个分支 。安全问题是执行时间行为难以追踪和理解 。GOTO语句可能会导致不希望的副作用，因为它们会中断特定 AP段的执行，而不能保证后续执行将满足使 AP进入该段的所有条件 。阻止或禁止此类应用程序编程实践的标准已经存在了二十多年 。通过消除 GOTO语句和使用适当的块结构 AP, 以最大化结构 。case、if.. . then. . . else、dountil和 dowhile语句结构允许使用定义的返回进行分支 ,并且不引入与 GOTO或等效语句相关联的控制流的不确定性 。

G. 3. 3. 3 控制流复杂性的最小化

控制流复杂性的一个指标是分支或循环的嵌套层数 。 过高的复杂度使得很难预测 AP 的流向 ,并妨碍审查和维护 。一个具体的安全问题是，当遇到非预期的参数组合时 ,控制流可能是不可预测的 。过度嵌套通常可以通过使用函数或子例程来代替内嵌分支来避免 。需定义嵌套的具体限制 ,作为项 目或组织编程指南的一部分，以解决安全问题 。

因此 ,IEC 61511将 AP架构中的层数限制为 2层：

- 典型逻辑;
- 联锁 。

IEC 61508-3适用于嵌套层数超过这一规定限制的 AP。

G. 3. 3. 4 使用前初始化变量

当变量在执行周期开始时未初始化为已知值 ,安全性会受到影响，因为它们可能包含“垃圾”值(该存储区内之前使用中留存的值) 。运行时可预测性要求将进程数据预留的内存存储区域在被访问(设置和使用)之前设置为已知值 。使用变量的未知初始值的具体结果取决于该变量在 AP 中的使用方 式 。IEC 61508-3适用于使用非初始化变量的 AP。

G. 3. 3. 5 子程序的单一入口和出口点

子程序中的多个进出点会导致类似于由 GOTO语句造成的控制流不确定性 。

通过对每个 AP设置一个入口和出 口，以增强运行时执行流的可预测性 。 因为执行流的可预测性是对安全性很重要的特性 ,所以子回路或函数中的多个入口和出口点是不可取的，即使语言支持它们 。IEC 61508-3适用于具有多个入口和出口点的 AP。

G. 3. 3. 6 最小化接口歧义

接口故障包括调用其他子程序 、与其他任务通信或在对象之间传递消息时参数列表不匹配 。这种错误的一个例子是在调用子回路时颠倒参数的顺序 。 以往对 AP失效的研究表明 ,这类故障是很常见的 。可以减少或消除接口故障可能性的应用程序编程实践包括：

- 对参数的数据类型进行交替排序(减少两个相邻参数按错误顺序排列的可能性)
- 对支持的语言(显 示) 命 名 的(参 数) 标 记 方 式，而 不 是 通 过 顺 序 或 位 置 的(隐 式) (参 数 标 记)

方式 。

- 在子程序开始时测试输入参数的有效性 。

程序需有充足的规定好的前置和后置条件 。前置条件确保所有局部变量都已初始化 ,并且所有输入变量都满足适当的合理性检查 。后置条件是所有输出变量满足适当合理性检查的保证 。

G. 3. 3. 7 使用数据类型(数据结构)

使用与 AP预期不同的数据结构可能会导致故障 ,并且在异常情况下发生的此类故障可能对安全性产生特别不利的影响 。这个问题可以通过声明数据类型来解决 。起初 ,声明数据类型的主要优点是允许编译器保留正确的内存量 。但是 ,数据类型对于改进接口的定义 、增加易读性(用于审查)以及编译时和运行时检查非常有用 。这些最初的辅助用途现在已经成为数据类型化的主要动力 ,并促进使用强类型强类型需要额外的声明 ,至少是有效范围的声明 。下面是与数据类型相关的安全问题 。

- 限制在强类型语言中使用匿名类型(例如 ,一般整数或无上限和下限的浮点) 。
- 确保对数据类型的限制不会受到过度约束 ,从而不会生成虚假的异常或错误消息(这在强类型语言中是一个问题) 。
- 最小化类型转换 ,并消除隐式或自动类型转换(例如 ,在赋值和指针操作中) 。
- 避免混合模式操作 。如果有必要进行此类操作 ,则需在 AP中使用突出的注释清楚地标识和描述这些操作 。
- 确保涉及算术求值或关系运算的表达式具有单 一 数据类型 ,是使转换难度最小化的适当的数据类型集合 。

将间接引用(例如 ,数组索引 、指针或访问对象)的使用限制在没有其他合理替代方案的情况下 ,并在设置或使用之前对间接寻址的数据执行确认，以确保访问位置的正确性 。强类型指针 、数组索引和访问类型减少了引用无效位置的可能性 。

G. 3. 4 考虑准确度和精度

G. 3. 4. 1 概述

AP的实现需为预期的安全应用提供足够的准确度和足够的精度 。 这既适用于物理特性的测量，也适用于 AP中的浮点运算 。 当分析不支持浮点变量的声明准确度时 ,尤其是当使用的大数之间的小差异时(例如，当计算当前值和以前值之间的差异的变化率时)计算方差或执行过滤操作(如移动平均) 。

G. 3. 4. 2 算术、逻辑和函数运算符的优先次序

算术 、逻辑和其他运算的默认优先顺序因语言而异 。开发人员或评审人员可能会做出错误的优先假设 。 因此 ,需使用机制确保明确说明了运算的求值顺序 。

G. 3. 4. 3 避免存在副作用的函数或程序

副作用是对该函数未返回的任何变量的更改 ,该更改在函数完成后仍然存在 。这包括对文件 、硬件寄存器等的更改 。这种副作用的一个例子是对不在函数参数列表中的全局变量的更改 。副作用会导致计划外相关性的问题 ,并且会导致很难发现的漏洞 。

G. 3. 4. 4 将赋值和求值分开

赋值语句宜与求值表达式分开 。 当子程序用作求值的一部分时 ,可能会违反这一分开原则 。例如，滤波函数可能被作为求值表达式的一部分而不是传感器的值 。一个相关的属性是尽量少用下面讨论的全局变量 。

G. 3. 4. 5　正确处理应用程序的辅助功能

AP插装在 AP执行期间收集并输出 AP的某些内部状态值，以使开发人员检查否正确实现了规范的特定方面 。具体的安全相关问题包括：

最小化运行时扰动:在安全应用程序中,干扰正常执行流的辅助函数是不可取的。 例如,大量的“写”或其他输出语句可导致执行与输出值相关联的大量库 AP;一 种干扰性较小的方法可能是将这些值写入外部存储器位置，以便稍后进行处理 。它还可能意味着以二进制格式写入数据以进行脱机格式处理(即 ,转换为人类可读的文本和数值) 。为了最大限度地减少测试和正常操作之间的行为差异 ,可能需要在实际环境中保持某些辅助功能 。

在运行时 AP中保持辅助函数的可见性 :一些 AP工具更改逻辑解算器生成的对象(或可执行文件)文档，以便插入辅助函数 。这在安全系统中通常是不可接受的，因为此类变更的影响在 AP 中是不可见的 ,并且其对执行的影响无法审查 。

遵循 AP辅助功能指南 :如果在项目专用的工程手册中描述了辅助功能的操作实践 ,那么审查会很方便(安全性也因此得到增强) 。这些指南宜确定需要使用什么类型的输出机制 ,并确定在哪些情况下不能使用这些输出机制 。例如 ,上文提到的 一 项用于减小对运行时干扰的措施，与附录 G 稍后描述的数据抽象和错误隔离属性并不一致 。

G. 3. 4. 6　控制类库的大小

控制类库大小对于避免系统变得不可管理或由于类和对象太多而导致性能下降非常重要 。如果项目特定的指导方针限制类和对象的数量,并且实际的AP符合这些指导方针,那么安全性就会得到增强。

G. 3. 4. 7　将动态绑定的使用降至最低

绑定表示名称与类的关联 。 动态绑定允许延迟名称/类关联，直到在执行时创建由名称指定的对象 。名称/类关联的不可预测性带来了安全问题 。它还降低了面向对象程序运行时行为的可预测性 ,并使调试 、理解和跟踪复杂化 。对于安全关键型应用程序 ,需要限制或避免动态绑定 。IEC 61508-3 适用于使用动态绑定的 AP。

G. 3. 4. 8　控制操作符重载

多态(操作符重载)允许对不同的数据类型使用单个子程序 、操作符或对象行为 ,从而提高可读性并降低复杂性 。然而 ,从可预测性的角度来看 ,它也可能是有问题的，因为不清楚逻辑解算器将如何为不同的多态绑定 AP(例如 ,多维数组上的乘法操作将如何绑定到标量或一维数组) 。

因此 ,项目特定或组织应用程序编程标准手册中对操作符重载的使用指南对安全相关应用是可取的，同时需验证 AP符合 GB/T 21109。

G. 3. 5　时间特性的可预测性

G. 3. 5. 1　概述

在用于实时控制的安全系统中 ,时间特性的可预测性是至关重要的 。 与此中间属性相关的面向对象编程的基本属性在前面的章节有描述：

- 控制类库的大小;
- 将动态绑定的使用降至最低;
- 控制操作符重载 。

以下子条款中讨论的与时间特性相关的两个额外的基本属性是：

- 尽量减少任务的使用;
- 尽量减少中断驱动处理的使用 。

G. 3. 5. 2 尽量减少任务分配的使用

尽管任务分配为并行处理提供了一个有吸引力的模型 ,但将它用于安全关键性应用是不可取的 ,原因如下：

- 当多个待调用任务等待执行时 ,执行顺序是不确定的，因为并不总是清楚将选择哪个调用;
- 任务分配允许出现诸如竞争条件和死锁之类的时间关键性错误。 这些问题很难通过调试解决 。

因此 ,除非有令人信服的理由 ,否则需避免在安全系统中使用任务分配 。

G. 3. 5. 3 减少中断驱动处理的使用

使用中断驱动处理来处理装置和操作员输入的接受和处理可以减少平均响应时间 ,但通常会导致不确定的最大响应时间 。在以往的事故中有一些与中断驱动处理有关 。

与数字系统安全相关的参考文件和标准通常不鼓励或禁止使用中断驱动处理(IEC 60880:2006) 。避免中断驱动处理有助于分析同步和运行时行为 ,并避免中断驱动处理固有的响应时间不确定性 。

G. 4 数学或逻辑结果的可预测性

可预测的数学或逻辑结果意味着在执行被检查的低级 AP时实现的结果是编写 AP的程序员预期的结果 。术语“逻辑”旨在将术语“结果”扩展到 AP操作布尔数据并将产生布尔结果的情况 。 因此 ,安全 AP宜是严格静态的。 GB/T 20438. 3— 2017适用于使用触发器存储器(无论是显式还是隐式)的 AP。

大量使用连锁改变了结果的可预测性 ,增加了 AP结构之间独立性证明的复杂性 。 SIF之间不宜互锁 。

计时器的使用宜受到限制 ,且不得级联或联锁 。

G. 5 鲁棒性

G. 5. 1 概述

鲁棒性是指 AP在非正常或其他非预期情况下继续执行的能力 。鲁棒性的同义词是生存性 。鲁棒性是安全系统的一个重要属性，因为意外事件可能在事故或漂移期间发生 ,AP在这种情况下继续监视和控制系统的能力至关重要 。

鲁棒性的中间属性为：

- 控制多样性的使用;
- 控制异常处理的使用;
- 检查输入和输出 。

G. 5. 2 控制多样性的使用

G. 5. 2. 1 概述

决定采用不同的 AP实现是设计层面的功能，因此不在本指南的范围内 。然而 ,如果在设计或要求中需要多样性 ,则需在其应用中加以控制 。在 AP中使用多样性的主要问题是 ,共模 AP故障可能导致冗余安全系统发生故障 ,从而导致安全功能丧失 。

独立开发的 AP进程之间共模失效的可能性不容易消除 。任何共享规范都可能导致共模故障 。 同样的问题也存在于开发测试数据来检查 AP的过程中,测试人员可能会忽略开发人员忽略的异常情况 。此外,为了使用能够实时比较 AP的多个变种的输出(或者能够比较中间结果)的方法,来自独立团队的设计可能受过度细致的规范约束 。这种详细的共用的规范可能导致 AP设计的多样性很小 。这在企业编程规范中很常见 。

另外,根据相同要求规范独立编写的多个 AP变种只对应用编程错误(有时仅对很有限的 一 部分编程错误)有效 。另一方面,实验证据表明,大多数安全问题(以及操作 AP 中发现的大多数错误) 都源于AP要求中的错误,特别是对 AP所要求操作的误解 。 图提供冗余的 AP可能无法实现目标,而只是重复了对需求的误解 。在审核安全关键 AP的过程中,对 AP多样性进行分析,以确定共模失效是非常重要的 。

有两个基本属性 :

- 控制内部多样性 ;
- 控制外部多样性 。

G.5.2.2 控制内部多样性

当只使用内部多样性时,所有变种的接口宜是相同的 。换句话说,来自调用程序的任何传感器数据或参数宜等同地传递给所有变种,并且来自任一变种的输出数据宜被系统的其他部分接受和使用 。然而,在各模块变种或例化中,对本地数据的内部操作和存储宜是不同的 。 内部多样性是由一个面向对象的方法来支撑的,在这个方法中使用相同的消息和方法,但是内部的算法和数据表示不同 。 内部多样性宜按照设计和项目具体指南实施,宜包括 :

- 多样化的算法:使用不同的算法 、单位转换和过程参数(当需求或设计中需要或允许时),将与设计或实现有关的失效的可能性降至最低 。
- 多样化的数据确认:对传感器(或其他输入)数据和输出数据确认使用替代方案,将与设计人员实现有关的失效的可能性降至最低 。
- 多样化的异常处理程序:该措施降低了在多个变种上同时发生异常处理或处理错误的可能性 。
- 多样化的数据类型 、结构和存储分配:该措施降低了由应用程序编程工具生成的对象 AP和逻辑解算器之间的意外交互将导致数据或 AP在多个变种上同时被无意覆盖的可能性 。
- 多样化的库和子进程:避免使用相同的 AP子程序 、编译器提供的库程序和逻辑解算器提供的应用程序编程接 口 。该措施降低了由于这些程序中的缺陷而导致同时发生故障的可能性 。
- 多样化的算术运算顺序:使用交换律 、结合律和分配律性质来改变转换 、算术和赋值语句中的算术运算顺序,降低了由于中间结果或数值精度问题产生的意外溢出条件而导致同时失效的可能性 。
- 输入和输出操作的多样化顺序:以不同的顺序执行 I/O操作可减少同时发生与时间相关的故障(如死锁)或数据驱动故障(即,由于特定数据值导致的 AP崩溃)的可能性 。

多样性的局限性在于,在一个给定的平台上,所有这些语言实际上只是相同算法的不同表示 。 因此,语言多样性的使用只会在汇编前缓解每种语言的弱点 。 因此 , AP可以用两种不同的语言编写 , 以比较它们的行为 。

G.5.2.3 控制外部多样性

在使用外部多样性的情况下,如果按照设计文件以严格的方式实施,安全性将得到加强 。设计文件需反映要求 、危害分析和类似来源所施加的多样性 。外部多样性是通过在变种之间使用不同的接口来实现的,也可以与内部多样性相结合 。 当不同的语言用于不同的变种时,外部多样性是必要的,并且也可以用于通过不同的通道获得传感器数据 。 由于难以维护 、测试 、验证和确认,不受控制或未规定的外

部多样性可能导致影响安全的接口扩散 。

G. 5. 3　控制异常处理的使用

G. 5. 3. 1　概述

异常处理过程用于处理异常的系统状态和输入数据 。某些语言中的异常处理规定有助于在出现意外情况时建立备用执行路径 ,从而进入提前定义的状态 。但是 ,在使用异常引发和处理时可能会出现问题，因为异常条件下的执行流通常很难跟踪 。

与异常处理相关的基本属性包括：

- 局部处理异常情况；
- 保持外部控制流；
- 异常的统一处理 。

G. 5. 3. 2　局部处理异常情况

在异常处理实现的位置 ,AP多个层次的次生异常可能使异常的确切状况被错误地理解 。 如果在局部处理好异常 ,就可以避免系统性失效(具有潜在的严重安全隐患) 。

G. 5. 3. 3　保护外部控制流

引发异常的程序的外部控制流被中断时 ,会在异常处理之后的执行过程中产生不确定性 。通过保护对异常情况负责的模块外部的控制流 ,可提高安全性 。

G. 5. 3. 4　统一异常处理机制

随意使用异常处理可能导致在 AP的不同部分对相同异常条件的处理不 一 致 。 最坏的情况是，它可能导致一些异常被引发而未被处理 。这些问题可以通过将异常处理使用指南作为组织或特定项目的应用程序编程实践规程的一部分来避免 。本指南包含的主题包括：

- 已定义并允许的通用的和项目专用的异常；
- 异常处理 AP的布置；
- 列举所有预期存在的副作用 ,并确认没有其他副作用；
- 异常处理过程中确保关键状态数据的完整性 。

区分哪些条件宜作为正常处理的一部分通过控制流构造来处理，哪些条件宜作为异常处理的 一 部分来处理的准则 。

G. 5. 4　检查输入和输出

G. 5. 4. 1　概述

由于瞬时失效或无效结果导致的数据损坏可能会对后续的处理造成严重的后果(如果允许扩散) 。与输入和输出检查有关的基本属性通过抑制该错误减轻其后果 。G. 5. 4. 2 和 G. 5. 4. 3 中讨论的两个基本属性为：

- 输入数据检查；
- 输出数据检查 。

G. 5. 4. 2　输入数据检查

输入数据包括来自另一个程序的数据 、来自外部环境的数据以及存储在内存中的来自上 一 次迭代的数据 。在处理之前 ,需检查输入数据的有效性 。这种检查降低了传播错误的结果或损坏的数据的可

能性 。需至少检查输入值的数据类型并在可接受的范围内 。 如有可能，还需对数据进行合理性检查 。AP中 宜存在检测无效输入的规定 ,并使模块达到更高级别设计中定义的已知状态(即默认值或先前有效值) 。

G. 5. 4. 3 输出数据检查

需检查输出数据的有效性 ,无论是到外部环境 、到另一个程序还是存储以供后续迭代使用 。此有效性检查至少需确保值为适当的数据类型 ,并且在可接受的范围内 。更可取的是 ,检查这些值的合理性 。然而 ,这样的合理性检查不宜限制性太强，以至于错误地拒绝正确的值 。AP 中还宜提供根据设计处理拒绝输出值的规定 。

G. 6 可追溯性

G. 6. 1 概述

如本附件前面所定义 ,可追溯性是指安全 AP支持针对 AP设计的正确性和完整性进行验证的属性 。可追溯性的中间属性是：

- 可读性;
- 控制内置函数的使用(G. 6. 2) ;
- 控制已编译库的使用(G. 6. 3) 。

由于可读性也是可维护性的一个中间属性，因此将在 G. 3. 4. 8 中讨论 。G. 6. 2 和 G. 6. 3 中讨论了后两个属性及其与安全的相关性 。

G. 6. 2 控制内置函数的使用

几乎所有语言都包含用于经常使用的编程任务的内置函数，以最大限度地提高程序员的工作效率 。然而 ,这些函数的局限性以及它们处理异常的方式可能不如基本语言结构的局限性那么为人熟知 。 因此 ,使用这些功能会引起安全问题 。

通过组织或特定项目指南 ,可以对使用内置功能产生的问题进行处理 。 回归测试用例可用于确定与新版本编译器和运行时间库预计结果的一致性 。 因此 ,需保留之前用于测试可容许内置功能的测试用例 、规程和结果 。测试还需评估特定运行环境内越界和边缘性条件(例如 ,关于平方根程序的负变元;字符串复制程序的不正确终止字符串)的行为 。

G. 6. 3 控制编译库的使用

编译库是由开发组以外的实体编写和编译的例程 。编译库的应用包括输入/输出操作 、设备驱动程序或标准语言中未定义的数学操作 。这些库可以由应用程序编程工具供应商 、第三方或开发组织的其他部门提供 。对此类库的关注点与对内置函数的关注点类似 。

通过组织或项目特定的指南来控制对这些库的函数调用的使用 ,可以解决对已编译库的使用的不确定性 。

与内置函数类似 ,需维护一组测试用例 、规程和结果 。测试用例需评估特定运行时环境中正常 、越界和边缘条件下的行为 。需为编译库的每个新版本执行回归测试 。

G. 7 可维护性

G. 7. 1 概述

AP可维护性降低了在进行更改时会引入错误的可能性 。 与可维护性相关的并会影响安全性的中间属性包括：

- 可读性 :AP便于项目人员理解 AP的属性;
- 数据抽象 :AP被划分和模块化的程度 ，以便将因 AP变化而产生的附带影响和意外副作用的可能性降至最低;
- 功能内聚性 :将设计级功能适当分配给 AP中的 AP设备(一个程序 ,一种功能) ;
- 延展性 :潜在变更的区域与 AP的其他区域隔离的程度;
- 可移植性 :其主要的安全影响是避免语言的非标准功能 。

G. 7. 2 可读性

G. 7. 2. 1 概述

可读性允许除作者之外的合格开发人员理解 AP。可读性对于可维护性的重要性可以通过 一 些研究看出 ,在发现应用程序编程错误方面 ,人工阅读 AP(桌面检查) 比结构或功能测试更有效 。 可以合理推断 ,可读性还将增强识别在纠正性或适应性维修期间要更改的 AP的能力 ,并降低在此类维修期间引入新故障的可能性 。

对于可读性 ,没有一个通用的标准可以强制执行甚至推荐 。但是 ,对 SIS需要组织或项目特定的应用程序编程风格和实践手册(或相关指南) 。 以下基本属性与可读性相关 。

- 符合缩进指南;
- 使用描述性标识符名称;
- 注释和内部文档;
- 限制子程序的大小;
- 最小化混合语言编程;
- 尽量减少晦涩难懂的编程结构;
- 尽量减少分散或相关设备;
- 减少字面常量的使用 。

G. 7. 2. 2 符合缩进指南

适当的缩进有助于识别 AP的声明 、控制流 、不可执行注释和其他设备 。缩进准则通常是项目特定或组织编程风格或标准的一部分 。缩进实践需要解决的重要问题是 :

- 编程块(由 begin和 end限定的语句序列) ;
- 注释;
- 分支结构(例如 ,if.. . then. . . else、case语句 、循环等) ;
- 多级嵌套(例如 ,do循环中的 do循环) ;
- 变量和子程序声明;
- 应用程序编程工具指南;
- 异常引发和处理 。

G. 7. 2. 3 使用描述性标识符名称

不易于理解的变量 、程序 、函数 、数据类型 、常量 、异常 、对象 、方法 、位号及其他标识符的名称可能会妨碍审核及维护 。 当要求这些名称具有可描述性 、一 致性 ,并可追溯至更高层级(即 AP设计) 的文件时 ,命名带来的安全性问题可得到缓解 。命名惯例是应用编程风格和实践手册的一个重要部分 。

涉及的问题示例包括 :

- 装置输入数据的标识(例如 ,变量是指向一个传感器 ,还是称为 loop1_hot_let_TC1) ;
- 如何命名循环变量(例如 ， “i,j,k” 或更长的标题) ;

- 标识符的本地重命名(例如 ,将“平均程序平均值”重命名为“平均值”);
- 区分不同类别的标识符(例如 ,在所有数据类型上都有一个后缀 ,用以区分它们与变量);
- 项目专用术语和保留字列表(例如 , 限制使用术语“报警”“限制”等)。

除非明显有利 ,否则需避免为不同目的使用相同的名称 ,并且在使用时 ,宜附有清晰 、一致和明确的标记 。多次使用同一个名称可能会造成混淆 。如果该语言支持预编译单元 ,也会存在问题 。在两个不同包中具有相同名称的变量(其中一个由另一个使用)可能被应用程序编程工具以不同于程序员预期的方式来解释 。在某些情况下 ,程序员可能忽略了包中名称的声明 。此时 ,另一个包可能会以完全非预期的方式使用具有相同名称的不同变量 。如果不经常遇到特定的分支或执行路径 ,则在导致运行时故障之前 ,可能不会发现此类故障 。

将保留字用于用户选择的标识符(在允许这一特征存在的语言中)是不可取的 。

G. 7. 2. 4 注释和内部文档

不完整的评论 、不一致的格式以及未更新以反映当前 AP 的注释妨碍了审查并引发安全问题 。 这些问题可以通过组织或项目应用程序编程规范的指导来最小化 ,这些规范控制注释和内部(AP) 文档 。合并后 ,需位于序言部分的项的示例包括 :

- 子程序或单元的目的及其实现方式;
- 功能和性能要求 , 以及子程序或单元支持实现的外部接 口 ;
- 调用的其他子程序或单元及其依赖关系;

全局和局部变量的使用 , 以及存储器和寄存器位置(如适用)以及具体维护说明;

- 负责编程的部门或科室;
- 单元的创建日期;
- 最新修订日期 、修订编号 、问题报告编号 、与修订相关的标题 、预期失效行为以及 AP所有主要部分的相关信息;
- 输入和输出 ,包括执行单元输入期间引用的数据文件;
- 关于每个参数的目的 、范围和限制的注释(对于带有参数的子程序) 。

AP 内文件的类似示例包括 :

— 在与数据类型 、变量和常量声明相关的注释中引用更高级别的设计文档;
— 分支和编程块开始时的目的和预期结果;
—详细的内嵌注释 ,解释不常见的构造和与编程实践的偏差 。

G. 7. 2. 5 限制子程序的大小

有些文件建议对每个子程序或单元的 AP进行特定的限制 。 例如 ,建议平均使用 100个不可扩展语句 ,最多使用 200多个这样的语句 。关注子程序的大小是采用结构化编程的动力之 一 。小规模的子程序(一 页或两页)比较长的子程序更容易检查 。但是 ,允许大小的限制还宜考虑程序和语言的性质 。在过程安全和控制系统中 ,一个给定的 AP需要经常处理大量感知的量 ,并且这些量的数据声明(带有所需的注释)本身可以超过一 页 。 因此 ,这个基本属性的准则是提供关于大小的指导 , 而不是 一 个通用的数字阈值 。

G. 7. 2. 6 减少混合语言编程

混合语言编程(例如 ,用于顺序控制的“顺序功能图”、用于布尔逻辑的梯形图和用于更复杂功能(缩放 、平均值等)的“功能块”给审查人员和维护人员带来了困难 , 因此是 一 个安全问题 。 当这种做法无法避免时 ,可以通过将“外来” AP放置在与其接口的主导语言例程(例如 , 与中断相关联的输入处理例程中的一个内嵌汇编应用程序编程工具指令)相邻的位置来尽可能减小此困难 ,从而增强可读性 。

当这种做法无法避免时，可以通过将“外来”AP嵌入与其接口的主导语言例程(例如，嵌入在功能块图的功能块中的结构化文本)中来尽可能减小此困难，从而增强可读性。

G. 7. 2. 7 减少不清楚或敏感的编程结构

模糊的应用程序编程结构通常可以描述为使用间接技术来减少实现结果所需的应用程序编程或逻辑解算器处理量。此类应用程序编程实践在审查和维护中存在问题，因此是一个安全问题。例如，向左移动一个整数相当于将其值加倍。然而，如果设计要求将值加倍(即，最好执行乘法)，则前一种构造将是模糊的;如果设计要求将值向左移动(即，最好在 AP 中执行移位操作，而不是乘以 2)。适当的注释可以最大限度地减少模糊或略微模糊的应用程序编程更改的影响(例如，将值自加作为使其加倍的手段)。

需避免通过“NOT”函数反转逻辑状态中的传感器或执行器实际状态，以及在整数和锁存输出中多路选择布尔值。

G. 7. 2. 8 最小化相关设备的分散

如果AP的相关设备分散在一个程序中，则在审查和维护期间需要参考AP列表中的多个位置。然而，分散的具体性质因语言而异。例如，一些语言允许从 AP主体中分离出接口规范;另一些则允许“原型”用于类似的目的。在具有强数据类型的语言中，可能需要将所有类型声明集中在一个文件(或一组文件)中;在面向对象语言中，可能需要将基类与派生类分开。如果提供有关 AP 中相关设备放置的项目特定指导，则有助于审查并提高安全性。

G. 7. 2. 9 减少字面常量的使用

字面常量(即 AP中的实际数字或字符串)比在模块开头为其分配常量值的名称更难识别。字面常量会影响安全性，因为它们会降低可读性，并使可维护性复杂化，特别是如果字面常量与可调的过程参数或可在重新校准仪表时更改的转换系数相关。更改文件开头的一个值集要比确保在所有相关文件中完全正确地更改与此类参数关联的所有文字要容易得多。

G. 7. 3 数据抽象

G. 7. 3. 1 概述

数据抽象是将数据和对该数据的允许操作组合到一个实体中，并建立一个只允许通过允许的操作访问、操作和存储数据的接口。通过减少或消除运行期间或 AP维护活动中改变变量的潜在副作用，实现对安全的重要贡献。此原则与以下具体基本属性相关：

- 尽量减少使用全局变量;
- 最小化定义允许操作的接口的复杂性。

G. 7. 3. 2 减少了全局变量的使用

在安全相关的程序中，最好限制全局变量的使用，因为有可能产生非预期的副作用。如果在同一个进程中设置和使用变量，可读性就会增强。这些变量可以通过已建立和控制的接口提供给其他例程，从而最大限度地减少意外交互的可能性。 出于同样的原因，宜避免或控制不同进程的内部存储数据之间的依赖关系。

为了避免潜在的安全问题，不同程序中的局部变量不宜共享相同的存储位置。

在 AP中，需避免使用可以从多个逻辑实例写入的全局变量，因为可能会产生意外的副作用。

G. 7. 3. 3　降低了接口复杂度

接口是 AP失效的常见原因 。复杂的接口很难审查和维护，因此在安全相关项 目 中并不可取 。 导致复杂性的特征包括：

- 调用例程时使用的大量参数;
- 在使用不同的模式或选项时 ,使用了过于简化的表达;
- 使用容许操作时 ,缺少易于理解的约束和限制条件 。

G. 7. 4　功能内聚性

G. 7. 4. 1　概述

功能内聚性是指AP的功能与其设备结构之间有清晰的对应关系。 功能内聚性只有一个基本属性。

G. 7. 4. 2　单一用途的功能和程序

当每个给定的进程 、子程序或功能只执行 AP设计中指定的 一 个任务或 目 的时，就 有 助 于 审 查 和维护 。

执行多个任务的子程序 、函数或进程宜分开 ,并作为单独的函数编写 。测试函数是否为单用途函数的一种简单方法是检查函数是否可以用以下形式的句子概括：

“动词 +对象”

IEC 61511期望典型逻辑被迭代 ,SIF被实现在单个逻辑解算器上 。

G. 7. 4. 3　单一用途的变量

单一用途功能的原理宜适用于变量 。一个变量只能用于一个用途 。

G. 7. 5　延展性

G. 7. 5. 1　概述

延展性是 AP适应功能需求变化的能力 。延展性扩展了数据抽象，目 的 是 隔 离 潜 在 变 化 的 区 域。为了实施一个可延展的 AP系统 ,有必要确定什么是预期不变的 ,什么是预期改变的 ,并将预期改变的部分隔离为易于识别的区域 ,这些区域的改变对附带区域带来的变动最小 。延展性只有一个基本属性 。

G. 7. 5. 2　可更改功能的隔离

隔离可更改的功能 ,使更改不影响其他 AP或数据，以便审查和维护 。 在许多情况下 ,这类功能是硬件相关的功能，当平台发生变化 、系统发生变化时 ,或者当使用新设备替换旧设备(例如 ,制造商生产的同一产品线的更强大的逻辑解算器)时 ,这些功能会改变 。

很大程度上 ,可更改功能的隔离是一个与数据抽象相关的设计问题 。正因如此 ,详细的讨论超出了本指南的范围 。

G. 7. 6　可移植性

G. 7. 6. 1　概述

从安全的角度来看 ,可移植性的好处是遵守标准编程结构 ,从而在不同的操作平台上产生可预测和一致的结果 。从而 ,复用或转换成在不同平台上运行的 AP将更易于维护 。 已经在其他地方讨论过的

与可移植性相关的属性包括：

- 尽量减少使用内置函数；
- 尽量减少已编译库的使用；
- 尽量减少动态绑定；
- 尽量减少任务分配；
- 尽量减少异步结构(中断) 。

唯一一个与可移植性相关的基本属性是避免使用专用于特定应用程序编程工具或应用程序编程工具与执行平台组合的非标准或“增强”构造 。

G. 7. 6. 2　非标准结构的隔离

如果需要非标准结构,需清晰地将它们与其基本原理、局限性和版本之间的依从关系一起识别出来 。

参 考 文 献

[1] GB/T 15969. 3— 2017 可编程序控制器 第 3部分 :编程语言

[2] GB/T 20438. 1— 2017 电气/电子/可编程电子安全相关系统的功能安全 第 1 部分 :一般要求

[3] GB/T 20438. 2— 2017 电气/电子/可编程电子安全相关系统的功能安全 第 2 部分：电气/电子/可编程电子安全相关系统的要求

[4] GB/T 20438. 3— 2017 电气/电子/可编程电子安全相关系统的功能安全 第 3 部分：软件要求

[5] GB/T 20438. 6— 2017 电气/电子/可编程电子安全相关系统的功能安全 第 6 部分：GB/T 20438. 2和 GB/T 20438. 3 的应用指南

[6] GB/T 21109. 2— 2007 过程工业领域安全仪表系统的功能安全 第 2 部分：GB/T 21109. 1 的应用指南

[7] GB28526— 2012 机械电气安全 安全相关电气 、电子和可编程电子控制系统的功能安全

[8] GB/T 35320— 2017 危险与可操作性分析(HAZOP分析)应用指南

[9] ISO 9000:2015 Quality managementsystems— Fundamentals and vocabulary

[10] ISO 10418: 2003 Petroleum and natural gas industries— Ofshore production instalations— Analysis，design，instalation and testing ofbasic surfaceprocessafety systems

[11] ISO TR 12489: 2013 Petroleum，petrochemical and natural gas industries— Reliability modeling and calculation ofsafety systems

[12] ISO 17776: 2000 Petroleum and natural gas industries— Ofshore production instalations— Guidelineson tools and techniquesforhazard identification and risk assesment

[13] ISO 31000:2009 Risk management— Principlesand guidelines

[14] IEC 60880: 2006 Nuclearpowerplants— Instrumentation and control systemsimportant to safety— Softwareaspects forcomputer-based systemsperforming category A functions

[15] IEC 61025:2006 Faulttreanalysis (FTA)

[16] IEC 61078: 2006 Analysis techniques for dependability— Reliability block diagram and boolean methods

[17] IEC 61131-3:2013 Programmable controlers— Part3: Programming languages

[18] IEC 61165:2006 Application ofMarkovtechniques

[19] IEC61506 Industrial-processmeasurementand control— Documentationofapplicationsoftware

[20] IEC 61882:2001 Hazard and operability studies (HAZOPStudies) — Application guide

[21] IEC62061:2005 Safetyofmachinery— Functionalsafetyofsafety-related electrical，electronic and programmable electronic controlsystems

[22] IEC 62502:2010 Analysis techniquesfordependability— Eventtreanalysis (ETA)

[23] IEC 62551:2012 Analysis techniquesfordependability— Petrinettechniques

[24] APIRP14C: 2001(R2007) Recommended Practice for Analysis，Design，Instalation，and Testing ofBasic SurfaceSafetySystemsforOfshoreProduction Platforms

[25] ISA TR84. 00. 02: 2002 Part 1 Safety Instrumented Functions (SIF) — Safety Integrity Level (SIL) Evaluation Techniques— Part 1: Introduction (note updated 2015 version below)

[26] ISA TR84. 00. 02: 2002 Part 2: SafetyInstrumented Functions (SIF) — SafetyIntegrity Level (SIL) Evaluation Techniques— Part 2: Determining the SIL of a SIF via Simplified Equations

(note updated 2015 versionbelow)

[27] ISA TR84.00.02:2002 Part3:SafetyInstrumented Functions (SIF) — SafetyIntegrity Level (SIL) Evaluation Techniques— Part3: Determiningthe SIL ofa SIF via FaultTre Analysis (note updated 2015 versionbelow)

[28] ISA TR84.00.02:2002 Part4:SafetyInstrumented Functions (SIF) — SafetyIntegrity Level (SIL) EvaluationTechniques— Part4: DeterminingtheSILofaSIF viaMarkov Analysis (note updated 2015 versionbelow)

[29] ISA TR84.00.02:2002 Part5:SafetyInstrumented Functions (SIF) — SafetyIntegrity Level (SIL) EvaluationTechniques— Part5: Determiningthe PFD ofSIS Logic Solvers via Markov Analysis (note updated 2015 versionbelow)

[30] ISA TR84.00.02:2015 SafetyIntegrityLevel (SIL) VerificationofSafetyInstrumented Functions ISBN:1-55617-802-6

[31] ISA TR84.00.03:2012 MechanicalIntegrityofSafetyInstrumented Systems (SIS)

[32] ISA TR84.00.04:2015 Part1:Guidelinesonthe ImplementationofANSI/ISA-84.00.01-2004 (IEC 61511)

[33] ISA TR84.00.09:2013 SecurityCountermeasures Related ToSafetyInstrumented Sys-tems (SIS)

[34] NFPA 85:2015 Boiler and combustions systems hazards code

[35] CCPS/AICHE Human Factors Methods forImproving Performance inthe Proces In-dustries (1stedition), JohnWiley & Sons (2007), ISBN 0 470117540

[36] CCPS/AIChE Guidelines forPreventing Human ErorinProces Safety (1st edition), JohnWiley & Sons (2004), ISBN 0816904618

[37] CCPS/AIChE Guidelines forChemical Proces Quantitative Risk Analysis (second edi-tion), New York: American Institute ofChemicalEnginers (2000),0 81690720X

[38] CCPS/AIChE GuidelinesforSafe AutomationofProcesApplications, 1993

[39] CCPS/AIChE GuidelinesforSafe Storage andHandlingofHighToxic HazardMaterial

[40] CCPS/AIChE GuidelinesforVaporReleaseMitigation

[41] CCPS/AIChE Guidelinesforthe TechnicalManagementofChemicalProcesSafety

[42] CCPS/AIChE Layer ofProtectionAnalysis, Simplified ProcesRisk Asesment, 2001

[43] HSE ReducingRisk ProtectingPeople, Health andSafetyExecutive, London(2001)IS-BN No. 07176-2151-0

[44] HSE Reducing eror andinfluencing behavior, HSG48, Health and Safety Executive, London(2009), ISBN 9780 717624522

[45] NAMURrecommendationNE130:2011, "Prioruse"-DevicesforSafetyInstrumented Sys-tems and simplified SILCalculation

[46] OSHA 29CFR 1910.119:2013, Processafetymanagementofhighlyhazardouschemicals