ICS 25.040
N 10

中华人民共和国国家标准

GB/T 21109.2—2007/IEC 61511-2:2003

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

Functional safety—Safety instrumented systems for the process industry sector—Part 2:Guidelines for the application of GB/T 21109.1

(IEC 61511-2:2003,IDT)

2007-10-11 发布　　2007-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB/T 21109《过程工业领域安全仪表系统的功能安全》分为三个部分：

——第1部分：框架、定义、系统、硬件和软件要求；

——第2部分：GB/T 21109.1的应用指南；

——第3部分：确定要求的安全完整性等级的指南。

本部分为GB/T 21109的第2部分，等同采用IEC 61511-2:2003《过程工业领域安全仪表系统的功能安全　第2部分：IEC 61511-1的应用指南》(英文版)。为便于使用，对IEC 61511-2:2003做了下列编辑性修改：

——删除国际标准的前言，按GB/T 1.1—2000重新编写了本部分的前言；

——凡是出现“IEC 61511”之处均改为“GB/T 21109”，“IEC 61511-1”均改为“GB/T 21109.1”，“IEC 61511-2”均改为“GB/T 21109.2”，“IEC 61511-3”均改为“GB/T 21109.3”；

——凡是出现“本国际标准”之处均改为“GB/T 21109”；

——用小数点“.”代替作小数点的逗号“,”；

——根据GB/T 1.1—2000进行编辑性修改。

本部分的附录A、附录B、附录C、附录D、附录E为资料性附录。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量和控制标准化技术委员会归口。

本部分主要起草单位：机械工业仪器仪表综合技术经济研究所、上海自动化仪表股份有限公司技术中心、北京华控技术有限责任公司、中科院沈阳自动化研究所、浙江中控技术有限公司、上海工业自动化仪表研究所、国营759厂。

本部分主要起草人：王春喜、梅恪、包伟华、王麟琨、刘丹、陈小枫、魏剑嵬、史学玲、谭平、李佳嘉、欧阳劲松、蔡廷安、马光武。

本部分为首次制定。

引　言

在过程工业(process industry sector)中,用来执行仪表安全功能的安全仪表系统已使用了多年。如要使仪表能有效地用于仪表安全功能,最重要的是该仪表应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 还要求执行一次过程危险和风险评估,来处理安全仪表系统和其他安全系统间的接口。安全仪表系统包括传感器、逻辑解算器和最终元件。

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。安全生命周期形成了核心框架,从而将本部分的大多数概念连接在一起。

安全仪表系统逻辑解算器包括电气(E)/电子(E)/可编程电子(PE)技术。在逻辑解算器使用其他技术的情况下,须应用 GB/T 21109 的基本原则。GB/T 21109 还涉及安全仪表系统的传感器和最终元件,而不管它们所使用的技术。GB/T 21109 在GB/T 20438—2006的框架范围内专用于过程领域(见 GB/T 21109.1—2007附录 A)。

GB/T 21109 提出了达到这些最低标准的安全生命周期活动的方法。为了使用合理和一致的技术策略,已采纳了此方法。本部分的目的是提供如何符合本部分的指南。

为了方便 GB/T 21109 的使用,提供的章、条号与GB/T 21109.1(附录除外)中对应的规范性内容相一致。

在大多数情况下固有(inherently)安全过程设计就能很好地实现安全性。必要时,还可结合一个或一些保护系统,以便处理任何已发现的残余风险。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、热力学的(如灭火器)、可编程电子的)。任何安全策略都需要将每个单独的安全仪表系统放在其他保护系统环境下进行考虑。为促成该方法,GB/T 21109 要求:

——执行一次危险和风险评估以便确定整体安全要求;

——给安全功能和相关安全系统(如安全仪表系统)分配安全要求;

——应在一个适用于所有用仪表实现功能安全的方法的框架内进行工作;

——详述了适用于实现功能安全的所有方法的某些活动(如安全管理)的使用。

关于过程工业的安全仪表系统的 GB/T 21109:

——涉及从初始概念、设计、实现、运行和维护直到停用的所有安全生命周期阶段;

——能使现有的或新的国家专用的过程工业标准同本标准协调一致。

GB/T 21109 致力于在过程工业领域内导致高度一致(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。

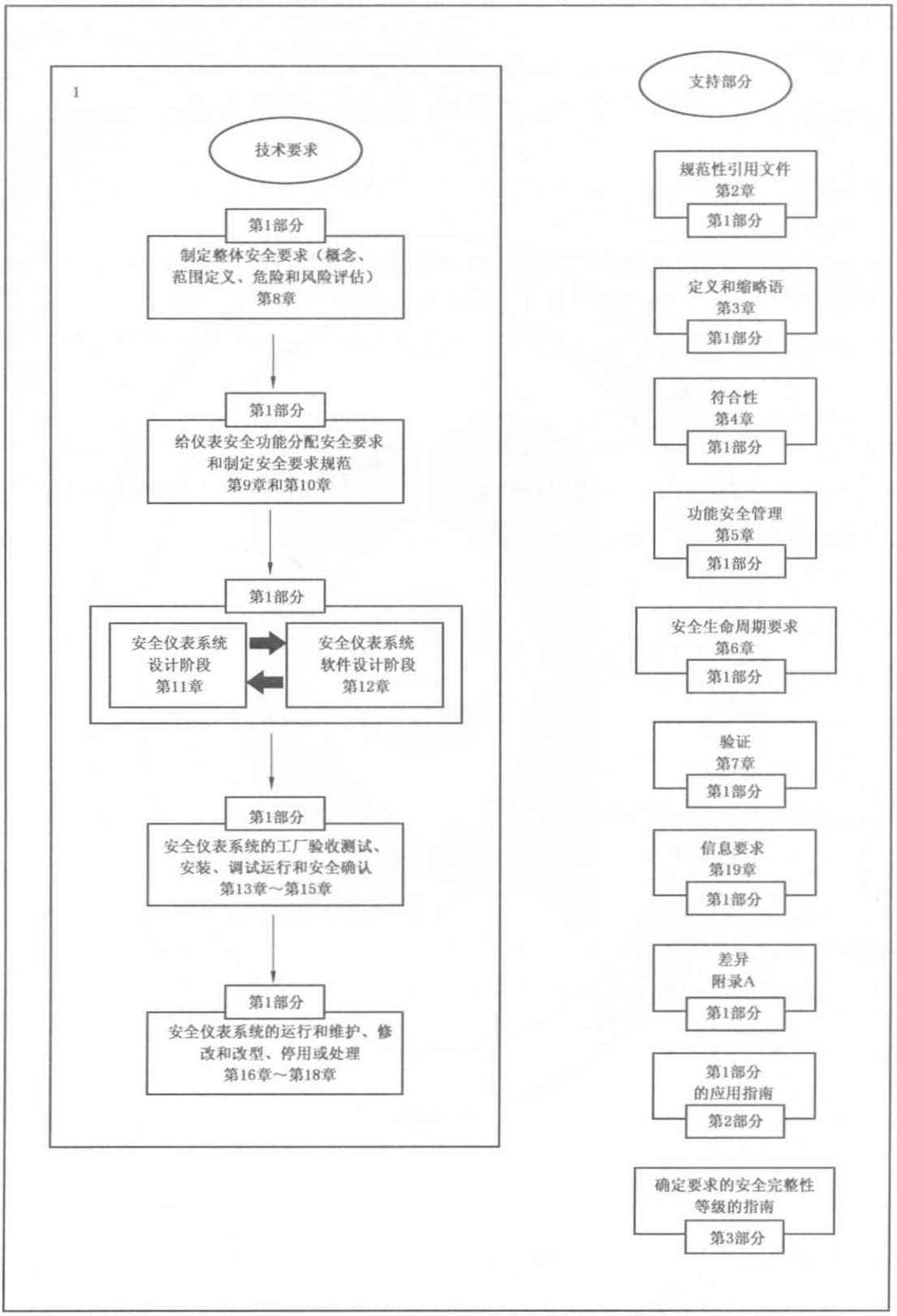


图 1　GB/T 21109 的整体框架

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的应用指南

1 范围

本部分提供了按GB/T 21109.1中定义的仪表安全功能及其相关的安全仪表系统的规范、设计、安装、操作和维护的应用指南。为了方便GB/T 21109的使用,提供的章、条号与GB/T 21109.1(附录除外)中对应的规范性内容相一致。

2 规范性引用文件

见GB/T 21109.1。

3 术语、定义和缩略语

术语、定义和缩略语见GB/T 21109.1。GB/T 21109.1—2007中以下两条术语在本部分中做了补充说明。

3.2.68

安全功能 safety function

一个安全功能应能防止一个特定的危险事件。例如"防止压力容器#ABC456中压力超过100 bar"。可以通过下列办法达到这个安全功能:

a) 单独一个安全仪表系统(SIS);或者

b) 一个或几个安全仪表系统和/或其他的保护层。

在情况b)中,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组合整体一定要达到要求的风险降低(过程安全目标)。

3.2.71

仪表安全功能 safety instrumented function

仪表安全功能源于安全功能,仪表安全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来执行它。例如"当压力容器#ABC456中的压力达到100 bar时,在5 s内关闭阀门#XY123"。多个仪表安全功能有可能使用同一个安全仪表系统的部件。

4 与GB/T 21109的符合性

见GB/T 21109.1。

5 功能安全管理

5.1 目的

GB/T 21109.1—2007第5章的目的是为保证满足功能安全目标必需实现的管理活动提供要求。

5.2 要求

5.2.1 概述

5.2.1.1 见GB/T 21109.1。

5.2.1.2 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,本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。但应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。

5.2.2 组织和资源

5.2.2.1 应定义一个公司/现场/工厂/工程项目范围内与安全仪表系统有关联的组织结构,并应清楚地了解和互通每个组成部分的作用和职责。应确定结构内的各个角色,包括它们的描述和目的。应清楚地标明每个角色的责任;并判明各自的特殊职责。此外,还应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它们对安全仪表系统而言所扮演的角色以及它们的职责。

5.2.2.2 应确定为实现与安全仪表系统有关的安全生命周期的任何活动所需的技能和知识;并应确定每种技能所要求的能力水平。应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,应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。当出现技术力量短缺时,可招收或签约合格的有经验人员。

5.2.3 风险评价和风险管理

GB/T 21109.1—2007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并未认同任何一种特殊的方法。换句话说,在GB/T 21109.3中鼓励读者就这一问题对这些方法进行复审。

5.2.4 计划编制

本条的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)。本部分未要求任何特殊结构用于这些计划编制活动,但它强调要求定期更新或复审这些活动。

5.2.5 实现和监视

5.2.5.1 本条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。

——确定SIS在它的整个工作寿命期内都能按安全要求规范运行。

5.2.5.2 在本部分中,供货商可能还包括设计承包商和维护承包商以及部件供货商。

5.2.5.3 应定期对SIS的性能进行复审,以保证在开发安全要求规范(SRS)过程中仍然遵守原来的设想。例如,应对SIS中的各个部件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,则有必要修改设计。同样还应对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。

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。评估者应对负责实现功能安全人员所作的决定作出判断。例如:在调试运行之前应对维护规程是否充分作一次评估。

功能安全审核人员应通过工程项目记录或者工厂记录来确定是否是具有必要资格的人员以规定的频率使用必要的规程。不要求审核者对它们考虑的工作的充分性作出判断。然而,如果它们发觉更改有益,则应在报告中包括对此的一个说明。

在许多情况下,评估者和审核者的工作之间有可能重迭。例如,一个审核者可能不仅需要确定一个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胜任能力作出判断。

5.2.6.1 功能安全评估

5.2.6.1.1 功能安全评估(FSA)的使用是证明一个安全仪表系统(SIS)满足仪表安全功能和安全完整性等级(SIL)要求的基础。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进行一次评估。为了进行一次有效的评估,应拟定一个定义该评估范围的规程以及评估组组成的指南。

良好的功能安全评估(FSA)惯例应考虑以下属性:

——对每个功能安全评估(FSA)都应拟制一个计划,这个计划应根据评估范围、评估人员、评估人员的能力以及评估将产生的信息来编排。

——FSA 应考虑到公司外部或者内部的标准、指南、规程或编程习惯(codes of practice)范围内所包含的标准和作法。FSA 计划应定义对于特定的评估/系统/应用领域应评估些什么。

——在不同的系统开发过程,功能安全评估的频次可能改变,但至少在系统面临潜在危险之前应进行一次 FSA。有些公司也可能在构建/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。

——在定义 FSA 频次和严密性时应考虑以下系统属性:

- 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。

——在评估之前应提供足够的设计、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。证据应代表系统设计或安装的当前/认可状态。

——评估者的独立性一定要合适。

——评估者应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 的方案都应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,可以使用检查列表来定义一个组织可接受活动的详细指南。

FSA 产生的记录应是完整的,并且在生命周期下一阶段开始之前,评估结论应同负责 SIS 功能安全管理人员的意见一致。

5.2.6.1.2 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、等级、职位)评估人员,以保证它们所关心的问题能被适时的关注和涉及。进一步建议,对于某些大型项目组或评估组,可能有必要拥有多个独立于初始项目组的高级人员。

根据公司组织结构和公司内部的专家意见,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,对于熟练进行风险评估及安全仪表系统应用的内部组织的公司可使用它们本身的资源来满足独立组织的要求,当然这样的内部组织应独立于负责项目的那些组织并在管理和其他资源方面是同负责项目的那些组织分开的。

5.2.6.1.3 评估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。在正在运行的工厂中改变不大的情况下尤其可能。

5.2.6.1.4 在某些地区,在阶段 3 进行的功能安全评估常被称为起动前的安全复审(Pre-Startup-Safety-Review(PSSR))。

5.2.6.1.5 见GB/T 21109.1。

5.2.6.1.6 见GB/T 21109.1。

5.2.6.1.7 评估组应能得到它们执行评估所需要的任何信息。这包括从设计阶段一直到安装、调试运行和确认阶段所作的危险和风险评估得到的信息。

5.2.6.2 **审核和修订**

5.2.6.2.1 本条给出有关审核的指南,并通过一个例子来说明相关活动。

a) 审核类别

安全仪表系统的审核可给工厂管理、仪表维修工程师和仪表设计工程师提供有用的信息。这使管理具有前瞻性,以及使之能了解它们的安全仪表系统的实现程度和有效性。存在有许多种能执行的审核类型。任何特殊活动审核的实际类型、范围和频率应反映该活动对安全完整性的潜在影响。

审核类型包括：

1) 审核，包括独立审核和自审核；

2) 检查；

3) 安全巡视(例如工厂走查和事故(incident)复审)；

4) 安全仪表系统调查(通过调查表)。

需要在“监督和检查”以及审核活动之间进行区别。监督和检查的重点在于评价特定生命周期活动的性能(例如在部件恢复工作之前，监督员检查维修活动的完成)。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安全仪表系统的实现上。一次审核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/工厂/项目的人员来执行(如自审核)，或由独立人员来执行(如公司的审核员、质量保证部门、调节员(regulator)、客户或者第三方)。

各级管理应使用相关类型的审核，以获取它们的安全仪表系统的实现有效性信息。来自审核的信息可用来确定可指导改进实现，但还未真正使用过的规程。

b) 审核策略

现场/工厂/项目实现审核的程序可以考虑滚动程序、独立程序或者自审核和检查程序。

应定期更新滚动程序，以便反映以往安全仪表系统的性能和审核结果，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/项目有关的所有活动和安全仪表系统的所有方面。

进行审核的主要原因以及它所产生的附加价值在于对它们提供的信息及时采取动作。这些动作的目的是增强安全仪表系统的有效性。例如，有助于降低雇员或成员公众受伤害或致命的风险、有助于提高安全文明、有助于防止任何应避免释放的物质进入环境。

总之，审核策略可以拥有各种审核类型的组合，它是由管理(客户)产生的、并为了把相关的信息反馈给管理链以便及时动作。

c) 审核过程和协议

总的目的是使审核的效能达到最大。仅当各方(包括审核者、联络员、工厂经理和部门负责人等)了解每个审核的需要并能影响每个审核时，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这些目的的方案的某种一致性。它们涉及审核过程的下列5个关键阶段：

1) 审核策略和程序

应清楚地定义每个审核的目的以及确定审核组以及每个组的任务和职责。

应有一个审核策略。

应有一个审核程序。

应对审核过程、程序和策略的实现进行复审。

2) 审核准备和预编制

开始进行某个审核之前，应为现场/工厂/项目的高级经理和/或适当的审核协调员确定一位联络员。

在早期阶段审核人员和联络员应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；

——需要参加的人员；

——审核的依据或者审核标准；

——为了增加审核的成功机率在准备阶段要作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%。

审核员应为审核收集信息、规程/指令等，以及在适当的时候准备数据和编制检查列表。

如果发现严重的观察结果/缺陷，审核员应强调和解释在审核过程中审核范围发生改变的可能性。

3) 实施审核

审核员应在对现场/工厂/项目人员可能造成的干扰具有足够的认识后，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，应定期向联络员通报，以免在审核结束时感到意外。

在审核过程中，审核员应设法接近工厂人员，以便将知识和理解(过程和审查结果的)通告给物主(achieve ownership)。

审核员的风格对审核的成功是决定性的——他应努力作到有耐心、态度积极、有礼貌、精力集中和客观。

至少审核员应力图作到在改变商定好的范围和时间表时需经协商。

4) 审查结果报告

在审核结束时或稍后，但应在发布最终报告之前，审核员应举行一个结束会议。

应给相关的管理部门提供对草案报告和审查结果提意见的机会，如有要求可在正式的结束会议上进行讨论。

通常的作法是请求现场/工厂/项目的一份行动计划，以便提交报告的审查结果。

5) 审核跟踪

通常审核报告要求用一份行动计划的形式作出回应。只要合适，审核员可在预定日期或者下次审核时，验证行动完成的满意程度。

现场/工厂/项目跟踪系统可用来检验行动计划的实现。

应考虑每个审核组的审核结果的定期复审/总结，并就其结果进行广泛沟通。

审核结果/输出可用于复审审核的频次，并可用于安全仪表系统的管理复审的输入。

5.2.6.2.2 本条增强了变更管理在审核过程中所起的作用。

5.2.7 SIS 配置管理

5.2.7.1 要求

5.2.7.1.1 为了在整个生命周期内管理和保持装置的可追溯性，可以建立一种用于标记、控制和追踪每个装置的型号/版本的机制。

在安全生命周期最早可能的阶段，应给每台装置标上一个独特的工厂标识。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，配置管理程序还应包括以下考虑。

配置管理系统可以包括：

a) 在生命周期的所有阶段，准备所有装置的标识规程。

b) 每台装置包括软件的型号/版本以及建造状况的独特标识，包括供货商、日期和应用地方、最初规定的型号/版本的变更情况。

c) 故障观察和审核产生的所有动作和改变的标识和跟踪。
d) 发布一个交付使用的版本的控制措施、标记相关装置的状况及型号/版本。
e) 已建立的安全防护措施,以确保在运行中的 SIS 不会遭受未经授权的变更/修改。
f) 每个软件项的版本标识,这些版本一起构成了一台完整装置的一个特定版本。
g) 提供在一个或多个工厂中多套 SIS 更新的协调。
h) 交付使用的书面授权。
i) 批准装置交付使用的一份签字批准的列表。
j) 阶段(stage/phase)装置被纳入配置控制之下。
k) 可交付使用的相关文档的控制。
l) 一台装置的每个型号/版本的标识:
——功能规范;
——技术规范。
m) SIS 的管理和维护涉及的所有部门/组织的确定、职责分配及其理解。

6 安全生命周期要求

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。针对一个安全仪表系统采用一种系统的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次序执行了这些活动。在GB/T 21109.1—2007的图 8 和表 2 中提出了一个典型的生命周期。在GB/T 21109.1—2007的第 8 章～第 16 章中给出了每个生命周期阶段的要求。

GB/T 21109 考虑了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。如果允许把安全活动较好地集成到常规的项目规程中,这种重新构建可能是有益的。GB/T 21109.1—2007的第 6 章的目的是当使用不同的安全生命周期时,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。

6.2 要求

6.2.1 考虑的关键是在事先定义将被使用的 SIS 安全生命周期。经验表明,除非事前对这个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了一致意见,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损害了安全。

6.2.2 虽然并没要求把建议的 SIS 安全生命周期(包括适用于项目的GB/T 21109.1—2007图 8 中的那些方框)映射到过程的项目生命周期上,但在某个早期阶段,这样做是有好处的。当作这件事时,应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。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。在这种情况下,有必要根据以往经验进行估计,然后在稍后的某个时候再证实这些数据。如果存在这种情况,那么在安全生命周期中注意这点是很重要的。

6.2.3 安全生命周期计划编制的另一重要部分是确定在每个阶段将使用的技术。确定这些技术是重要的,因为通常需要使用某个专门的技术,这种技术要求人员或部门要具有独特的技能和经验。例如,在某个特定应用中的后果可能与失效事件后形成的最大压力有关;能够确定这种关系的惟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对设计过程将有重大影响。

7 验证

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,还是硬件和软件形式)已被产生且适合它们的用途。

7.1.1 要求

7.1.1.1 GB/T 21109.1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，本条的目的是在事先就计划好所有的验证活动，连同任何会被使用的规程、措施和技术。

7.1.1.2 见GB/T 21109.1。

7.1.1.3 提供验证结果是重要的，这样可以证明在安全生命周期的各个阶段都已进行了有效的验证。

8 过程危险和风险评估

8.1 目的

本章的总体目标是确定用以保证过程安全所需的安全功能(如保护层)，及其相关性能水平(风险降低)。在过程领域中，使用多个安全层是常见的，这样在某一层失效时才不会导致或者允许产生有害的后果。在GB/T 21109.1—2007的图 9 中表示了典型的安全层。

8.2 要求

8.2.1 只能根据任务的结果来规定危险和风险评估的要求。这意味着组织可以使用它认为有效的任何技术，只要该项技术能得到安全功能及其相关性能水平的清楚描述。

危险和风险评估应确定和涉及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)发生的危险和危险事件。

就过程领域的一个典型工程项目而言，需要在基本过程设计的初期就执行预先的危险和风险评估。在此阶段假设通过固有安全原理以及好的工程实践的应用，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(在 GB/T 21109 的范围内不包含这种降低危险的活动)。对 SIS 而言，这种预先的危险和风险评估是很重要的，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。及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结构方面的信息。

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，启动预先危险和风险评估的信息就足够了。应该认识到当进行详细设计时，可能引入附加危险。因此，一旦完成了过程和仪表图，还有必要进行一次最终的危险和风险评估。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)。应证实所设计的安全层足以保证工厂的安全。在该最终分析期间，需考虑安全系统的失效是否会导致任何新的危险或者请求。如果在此阶段确定有任何新的危险，则有必要定义新的安全功能。另一较可能产生的结果是查明了可导致在初始阶段已识别危险的附加事件。于是需考虑是否需要对初始分析所确定的安全功能及其性能要求进行修订。

用来确定危险的方法取决于正在考虑的应用，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)具有广泛操作经验的情况下，使用工业上编制的检查列表(例如 ISO 10418 和 API RP 14C 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，有必要采用一种更结构化的方法(例如 IEC 60300-3-9:1995)。

注：ISO 17776 中给出了有关选择合适技术的其他信息。

当考虑特定失效事件的后果时，应分析所有可能的结果，及对结果产生影响的失效事件的频率。在风险分析中应忽略或去除不可靠的结果。使管道或压力容器承受超过设计的压力不一定会产生灾难性的污染损失。在许多情况下，设备都经过超过设计的压力试验，惟一可能导致火灾的后果是可燃物质的泄漏。在评价后果时，需咨询负责工厂机械完整性的人员。它们不但需要考虑原始试验压力还要考虑包括腐蚀允许量在内的原始设计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，清楚地讲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，另外一个问题是许多人可能会受到某种特殊危险的影响。许多情况下，操作和维护人员只是偶尔在危险区域出现，在预测后果时应考虑到这一点。在使用这种统计方法时应注意并非对所有的情况它都有效，比如只是在起动期间才发生危险以及人员经常出现在危险区的情况。还应考虑到由于在事件的发生过程中要

对征兆进行调查，所以在危险事件附近出现的人数还可能增加。

当对 SIS 的潜在要求源进行评估时，评估应包括以下情况：起动、连续操作、停机、维修错误、手动干预(如手动控制器)、供应的中断(如空气、冷却水、氮、动力、蒸汽、加热保温层等)。

当考虑要求频率时，在某些复杂情况下，可能有必要进行一次故障树分析。仅在因多个事件的同时失效而产生严重后果的情况下(例如，未为所有泄压的最坏情况设计减压收集器)，这经常是必要的。应对什么时候应把操作员错误包含在可能引起的危险事件，以及这种事件发生的频率的事件清单中做出判断。如果操作员动作需经允许规程或者开锁设施(为防止偶然动作而配备的)才能执行，那么通常就可排除操作员错误。还需注意的情况是在什么场合，由于操作员动作降低要求频率是可信任的。这种信任会受到人为因素(比如需要多快地采取动作)和涉及任务的复杂程度的限制。在操作员对报警采取动作以及所声明的风险降低因子大于 10 的情况下，则需要根据GB/T 21109.1设计整个系统。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、人工响应以及操作员用来消除任何危险的设备。声明的风险降低因子不大于 10 的情况无需遵从 GB/T 21109，这时应仔细考虑人为因素问题。由于报警而降低风险的任何声明必须得到三个方面的支持：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的时间，保证操作员采取预防动作的培训。

倘若下列条件成立，降低对 SIS 的要求率就能把一个报警系统用作一种风险降低的方法：

——当失控将导致对 SIF 的一次要求时，用于报警系统的传感器不用作控制目的；

——用于报警系统的传感器不用作 SIS 的组成部分；

——已经考虑到关于风险降低的限制，这种风险降低可被声明用于 BPCS 和共同原因问题。

GB/T 21109.3给出了可用来确定安全仪表系统的 SIL 的技术示例，还包含在选择用于某个特定应用的方法时需考虑哪些问题的指南。

当确定是否需要风险降低时，需要具有一些过程安全和环境目标。它们专用于特定的现场或操作公司，并且可同未使用附加安全功能的风险水平进行比较。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某个安全状态。理论上，可以用通用术语描述这些功能而无需涉及某个特殊技术。例如在过压保护的情况中，可把功能描述成防止压力上升超过某个规定值。无论是一个安全阀或是一个安全仪表系统都能执行此功能。当如上描述功能时，则可在生命周期的下一阶段(给保护层分配仪表安全功能)来决定所使用的技术类型的选择。实际上，根据所选的系统类型，功能要求是不相同的；在某些情况下，此阶段和下一阶段可结合起来。

总之，危险和风险分析应考虑：

——每个已确定的危险事件和导致该危险事件的事件序列；

——与每个危险事件相关联的事件序列的后果和可能性，可定量或定性表示它们；

——每个危险事件的必要的风险降低；

——为降低或消除危险和风险而采取的措施；

——在分析风险过程中所作的假定，包括估计的要求率和设备的失效率，应详细说明操作约束或人为干预取得的任何信任；

——在每个 SIS 生命周期阶段(如验证和确认活动)对与安全相关系统有关的关键信息的引用。

构成危险和风险分析组成成分的信息和结果都应文档化。

当已经做出了决定并且可用的信息变得更精确时，可能有必要在整个 SIS 安全生命周期的各个阶段反复进行危险和风险评估。

8.2.2 在过程工业中，在许多应用中需考虑要求的一个重要理由是 BPCS 失效。传感器、阀或控制系统都可能引起 BPCS 失效。

在过程工业中使用的控制系统有时具有冗余处理器，传感器和阀一般没有冗余。当给 BPCS 分配一个失效率时，需要知道失效率有一个重要限制。GB/T 21109.1对与某个特殊危险有关的危险失效率作了限制，即除非系统的实现符合该标准的要求，能声明的危险失效率只能到每小时 10^{-5}。这种限制

的理由是如果声明的危险失效率较低，它应是在GB/T 21109.1—2007表4的失效率范围之内。此限制保证了不满足GB/T 21109.1要求的系统不会有高的置信度水平。

8.2.3 见GB/T 21109.1。

9 给保护层分配安全功能

9.1 目的

为了确定所需的SIS和相关的SIL，考虑现有一些(或需要有些)什么样的其他保护层以及它们所提供的保护功能有多大是很重要的。在考虑了其他保护层之后，应对SIS保护层的需要作出判定。如果需要一个SIS保护层，则应确定该SIS的仪表安全功能的SIL。

9.2 分配过程的要求

9.2.1 本条的要求是商定将使用的安全层和分配仪表安全功能的性能目标。实际上，在许多情况下，只有在使用固有的安全设计或其他技术系统存在问题的场合，才将安全功能分配给安全仪表系统。

这类问题的例子包括对燃烧容量的限制或者针对放热反应的保护。使用基于仪表的系统而不是像安全阀这类更传统方案的任何决定，都需要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，危险和风险评估与分配可能同时进行；在某些情况下，分配可以在危险和风险评估前进行。决定给安全层分配安全功能通常应根据用户组织发现是切实可行的依据做出。还应考虑已确定的良好的行业惯例。然后在假定其他安全层是可信任的情况下，对安全仪表系统做出判定。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，安全仪表系统仅用于限制压力。

9.2.2 见GB/T 21109.1。

9.2.3 在把一个安全功能分配给一个仪表安全功能时，需考虑应用是以要求模式还是以连续模式操作。过程领域中的大多数应用在要求不是很频繁的情况下都使用要求操作模式。在这类情况中，GB/T 21109.1—2007的表3是常用的合适量值。有些应用要求很频繁(例如要求率每年大于1)，这类应用更适合当作连续模式，因为危险失效概率主要是由SIS的失效率决定的。在这些情况下，宜使用GB/T 21109.1—2007表4中的适当量值。失效导致即时危险，在连续模式中是很少见的。如果对于控制系统的所有失效模式而言，保护系统不能满足要求，燃烧器或汽轮机速度控制就可采用连续模式应用。

GB/T 21109.1—2007的表3中SIL是通过PFD_{avg}来定义的。而目标PFD_{avg}是通过要求的风险降低来确定的。要求的风险降低能通过对没有SIS时的过程风险同允许风险进行比较来确定的。它能够通过GB/T 21109.3中的技术按照定量或定性的原则来确定。

GB/T 21109.1—2007的表4用执行SIF的危险失效目标频率来定义SIL。可通过SIS的允许失效率并考虑特定应用中失效的后果来确定SIL。当使用GB/T 21109.1—2007的表4来确定要求的SIL时，目标会基于安全仪表系统的危险失效频率。在使用GB/T 21109.1—2007的表4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，但这会导致GB/T 21109.1—2007的表4的不恰当转换，并可能导致安全功能的SIL要求的不规范。

要求时的平均失效概率目标或者每小时的危险失效频率目标适用于仪表安全功能，并不适用于单个部件或子系统。一个部件或子系统(如传感器、逻辑解算器和最终元件)除了它被用于某个特定SIF之外，不能给它指派一个SIL。但它具有独立的最大SIL能力的申明。

危险和风险评估和分配过程的输出，应该是安全系统所执行功能的一个清晰的描述，包括潜在的安全仪表系统及其所有仪表安全功能的安全完整性等级要求(连同操作模式——连续或要求)。它构成了SIS安全要求规范的基础。应清楚地描述确保能维持安全所需要执行的功能。

在此实现阶段,不必规定传感器和阀门的架构的细节。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。

9.2.4 需要完全了解GB/T 21109.1—2007中表 3 和表 4 的含意。特别是,单个仪表安全功能可以声明的 PFD_{avg} 限制到 10^{-5},这相当于 10^5 的风险降低(SIL 4)。可靠性分析指出由于硬件随机失效的 PFD_{avg} 小于 10^{-5} 是可以达到的,但GB/T 21109.1认为系统失效和共同模式失效会限制实际可能达到的性能。强烈推荐在风险分析显示出需要高的风险降低的情况下,应注意到过程领域中要达到 SIL 4 的仪表安全功能是困难的。解决办法是使用几个较低完整性的独立 SIS。

根据GB/T 21109.1—2007的 9.2.4 的注 4:

为了达到较高的风险降低水平(如大于 10^3),可以使用多个 SIS。当使用多个 SIS 来达到较高的风险降低时,重要的是每个 SIS 应能独立地执行安全功能,并且各 SIS 之间应有足够的独立性。例如,把一个 SIL 2 的压力检测回路同一个 SIL 1 的液位检测回路组合起来,以达到具有 10^3 风险降低要求的过压安全功能也许并不可取;因为液位传感器检测到一个高液位之前,压力容器就可能已经超过了它的压力限值。

另外,在使用多个 SIS 时,还应考虑共同原因失效。此外,还要满足GB/T 21109.1中定义的所有其他要求,包括表 5 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 SIS 来达到较高的风险降低水平,考虑下例:

一个由 2oo3 变送器组、一个 2oo3 逻辑解算器和一个 1oo2 最终元件组构成的一个具有 PFD_{avg} 为 3.05×10^{-4} 的 SIS。该 SIS 达到的风险降低大约为 3.3×10^3。

假定使用两个这样的系统来产生一个 10×10^6($3.3\times10^3\times3.3\times10^3$)的风险降低是不正确的。共同原因因素(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、空气管道的冻结、闪电)都将限制系统提高。还有必要考虑两个系统间任何共享的部件。

一种较可行的解决办法是使用尽可能多样性的部件(为了最小化潜在的共同原因问题)的一个非冗余第二系统。

例如,考虑包含仅一个开关、继电器逻辑和仅一个最终元件的系统,该系统具有一个 7.7×10^{-3} 的 PFD_{avg}。此系统达到的风险降低大约为 1.3×10^2。

把基于软件的 SIS 和单纯继电器型 SIS 组合起来,可得到的总体理论风险降低为 4.3×10^5($3.3\times10^3\times1.3\times10^2$)。如上所述,尽管在理论上性能的组合似乎是可能的(因为无论哪个 SIS 都能使过程单元停机),但同样不得不考虑共同原因因素,并且由于这些因素使之可达到的风险降低要稍微低一点。

9.3 安全完整性等级 4 的附加要求

9.3.1 见GB/T 21109.1。

9.3.2 见GB/T 21109.1。

9.4 作为一个保护层的基本过程控制系统的要求

9.4.1 基本过程控制系统也可视为是一个遵从某些条件的保护层。如果在 BPCS 中,以降低过程风险为目的的功能得到实现,针对预定要降低的确定的风险,也可给 BPCS 分配一个风险降低。

9.4.2 不需遵从GB/T 21109.1,仅表型系统就可声明低于 10 的风险降低。这使得 BPCS 可用于某些风险降低,而无需按GB/T 21109.1的要求实现该系统。应通过考虑 BPCS 的完整性(由可靠性分析或者性能数据确定)和用于配置、修改、操作和维护的规程表证明所作的任何声明都是合理的。当在 BPCS 中给功能分配风险降低时,保证提供访问保密和更改管理是重要的。能声明的一个 BPCS 功能的风险降低也可由 BPCS 功能和诱发原因之间的独立程度来确定。图 2 说明了 BPCS 功能和诱发原因之间的独立性。

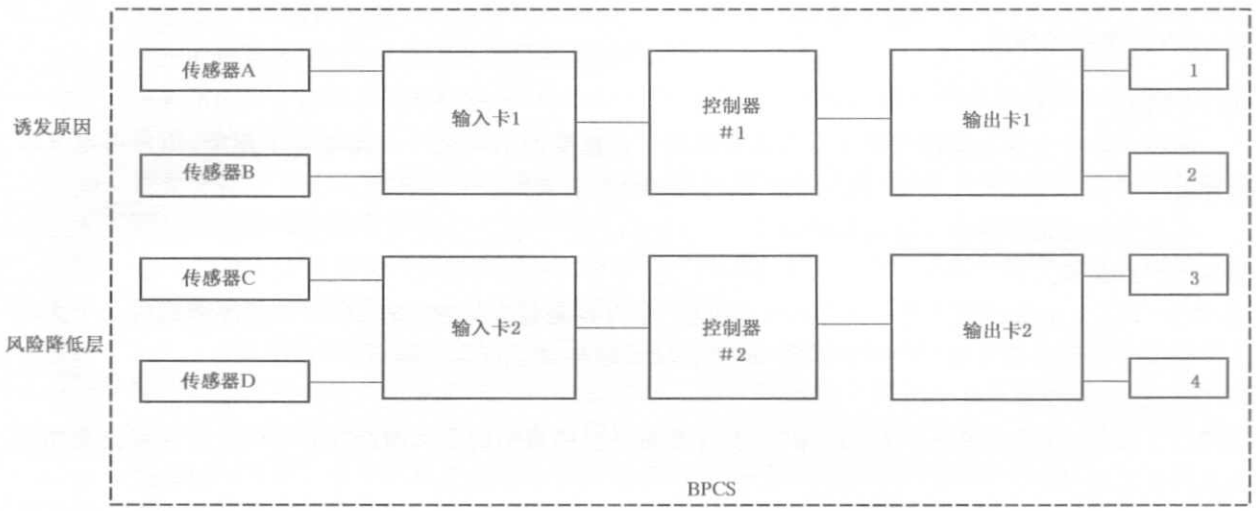


图 2　BPCS 功能和诱发原因的独立性说明

例如，考虑一个流量控制回路是诱发原因的情况。此诱发原因包括一个流量变送器、一个控制器和一个控制阀。为了给 BPCS 中的一个压力控制回路分配风险降低，压力变送器应连接到一个独立的控制器，调节一个独立的最终元件(例如到燃烧系统的排气阀)。

9.4.3　见GB/T 21109.1。

9.5　防止共同原因失效、共同模式失效和相关失效的要求

9.5.1　在早期阶段应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 2 个安全阀之间)、各安全层之间或者各安全层和 BPCS 之间是否存在任何共同原因失效。一个基本过程控制系统测量的失效可能引起对安全仪表系统提出一次要求，以及在安全仪表系统中使用一个具有同样特点的设备的情况就是它的一个例子。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。在判明是一个共同原因失效的情况下，则可采取以下动作：

a)　可通过改变安全仪表系统或者基本过程控制系统的设计来减少共同原因。降低共同原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应考虑共同原因事件的可能性。这要求对由要求原因以及保护系统失效构成的故障树进行一次分析。在这种故障树上可以表示出共同原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 共享的任何传感器或者执行机构都很可能引入共同原因失效，而解决装置的这种共享的方法应如本条中所述。

9.5.2　当对共同原因失效、共同模式失效和相关失效的可能性执行一次评估时，应使用下面所列的考虑。评估的范围、形式和深度取决于预期功能的安全完整性等级。对安全完整性水平为 3 或者更高的情况而言，共同原因、共同模式和相关失效的影响也许是决定性的。应考虑：

——各保护层之间的独立性：应进行一次失效模式影响分析，以便确立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：目标应是各保护层和 BPCS 之间的多样性，但并不一定总是能作到。例如过压保护，在这种情况中，BPCS 压力控制回路的一次失效将导致一次要求。BPCS 和 SIS 都需要测量压力，并对提供的合适设备有一个限制。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 传感器连接到过程，则多样性也许很有限。

——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同原因失效的影响。根据比如精确性和响应时间这样的功能需要，BPCS 和 SIS 的测量连接位置应有最大物理间隔。

10 SIS 安全要求规范

10.1 目的

拟制 SIS 安全要求规范是整个安全生命周期中很重要的活动之一。通过这个规范，用户可定义应怎样设计需要的仪表安全功能(SIF)和如何把这些功能集成到一个 SIS 中。

应使用此规范来执行 SIS 的最终确认。

10.2 一般要求

10.2.1 SIS 安全要求规范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。可由危险和风险评估组和/或工程项目组本身拟订这些要求。

10.3 SIS 安全要求

10.3.1 如GB/T 21109.1中描述的那样，有许多需要在项目初期定义的设计要求以确保仪表安全功能提供所要求的保护。

各个子系统的安全要求规范也可从这个总体规范中推导出。

有关安全要求规范的一些考虑如下：

a) 需定义的首要条款是仪表安全功能及其安全完整性等级(SIL)。一个仪表安全功能的例子是“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：

——检测危险工况征兆需采取的测量。一个简单的例子可能是检测压力上升超过某个规定值。当压力处于某参数值时应采取动作，该参数值需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现安全仪表系统的人员进行讨论。

——防止危险工况需要采取的动作。一个简单的例子可能是在规定的时间内减少流到重沸器(reboiler)的蒸汽流量。应注意的是，一般仅说明应切断流到重沸器的蒸汽流还是不够充分的。设计师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牢牢地关断蒸汽流。

——不是为了防止危险工况的需要而是可能有利于操作采取的动作。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提出要求，或者减少一旦消除了危险的起因则使能快速起动的动作。值得注意的是，应把这些动作同为防止危险工况的必要动作分开，以便最小化成本和把安全仪表系统的边界限定到必要范围内。边界设定越宽，在要求时的整体失效概率满足与规定的完整性等级相关的要求就显得越困难。

——避免任何已识别出的可导致危险情况的过程状态或者 SIS 操作顺序。

——任何由于会导致危险情况而需要被防止的已识别出的过程状态或者 SIS 操作序列。

b) 根据应起动或停止哪个流程、应打开或关闭哪个过程阀门以及任何旋转设备(泵、压缩机和搅拌器)的操作状态，本规范应定义每个已识别出的功能的过程安全状态。如果将一个过程导向安全状态涉及顺序要求，则也应确定该顺序。

注：在定义最终元件时，应考虑多样性的好处，例如，关断产品流和关断蒸汽流以降低高压。

c) 在开始设计 SIS 时，就应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，如果要在计划的停机期间(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。

d) 应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，则需对此进行规定。也需规定 SIS 逻辑解算器的手动停机开关的任何独立性要求。

e) 需规定在一次停机之后重新起动过程的所有要求。例如，某些用户在主控面板上或在现场有

电子复位开关，而另有一些用户则可能使用带锁定手柄的螺线管。如果存在类似于这种复位动作的特殊要求，它应是安全要求规范的组成部分。

f) 如果存在一个伪脱扣的目标频率，也应把它作为安全要求规范的一部分进行规定，它将是SIS设计中的一个因素。

g) 需充分描述SIS和操作员之间的接口，包括报警(预停机报警、停机报警、旁路报警和诊断报警)，图形和事件顺序记录。

h) 也可能存在旁路需要以便能在过程运行的同时测试或维护SIS。如果存在旁路诸如键锁或口令这类装置的特殊要求，也需要把这些作为安全要求规范的一部分规定下来。

i) 应定义SIS的失效模式和对已检测到的故障的响应。例如，可以把一个变送器设计成失效就面临一次脱扣状态或者失效就解除脱扣状态。如果把它设计成失效就解除脱扣状态，重要的是操作员能得到变送器失效的一个报警以及培训操作员采取必要的纠正动作，以使变送器尽快地得到修复。关于已检测出的故障的要求，见GB/T 21109.1—2007的11.3。

10.3.2 见GB/T 21109.1。

11 SIS设计和工程

11.1 目的

本章的目的是提供SIS的设计指南。每个SIF都有它自己的一个SIL。SIS的一个部件，如一个逻辑解算器可以被不同SIL的若干个SIF使用。

11.2 一般要求

11.2.1 见GB/T 21109.1。

11.2.2 见GB/T 21109.1。

11.2.3 见GB/T 21109.1。

11.2.4 GB/T 21109.1—2007的第11章有许多SIS的设计要求。其中一项是SIS和BPCS之间的独立性。

通常因以下原因，SIS是同BPCS分开的：

a) 为了降低BPCS对SIS的影响，特别是当它们共享共用设备时。例如，当BPCS和SIS共享一个用于停机和控制的共用阀门时，在该阀门的一次危险失效事件中，它并不能用来执行一个SIS停机功能。

b) 为了保持与BPCS有关的更改、维护、测试和文档的灵活性。

注1：通常SIS比BPCS有更为健壮的要求，而且不会要求BPCS具有和SIS一样的健壮要求。但应注意，不受控制的BPCS修改可能造成对SIS提出更多的要求。

c) 为了有助于SIS的确认和功能安全评估。

d) 如果BPCS与SIS组合在一起，为满足修改管理的计划安排，需要限制对BPCS的编程和配置功能的访问。

在共用设备的一次失效可引起向SIS提出一次要求的情况下，应进行一次分析以保证总危险率满足预期值。总的危险率是共用元件的危险失效率和其他要求源的危险率(包括SIS独立部分的危险失效)的总和。

SIS和BPCS之间的分离可使用同种分离或异种分离。同种分离意味着BPCS和SIS使用相同的技术，而异种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种分离相比，异种分离有利于降低系统失效概率和减小共同原因失效。

在SIS和BPCS之间的同种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部件。

虽然要考虑共同原因失效的源头和影响，并且要降低它们的可能性，但对SIL 1、SIL 2和SIL 3而

言,SIS 和 BPCS 之间的同种分离是可接受的。共同原因失效的一些例子是:

a) 仪表连接器的插拔和导线上的脉冲群;

b) 侵蚀和腐蚀;

c) 由于环境引起的硬件故障;

d) 软件误差;

e) 动力源和供电;

f) 人为误差。

异种分离有助于降低系统失效概率(在 SIL 3 和 SIL 4 应用中此降低因子特别重要)和减小共同原因失效。

一般可供 SIS 和 BPCS 进行分离的区域有 4 个:

1) 现场传感器;

2) 最终元件;

3) 逻辑解算器;

4) 配线。

BPCS 和 SIS 之间也不一定需要物理分离,其条件是它们之间应保持独立性,并且设备安排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。

SIS 设计师需规定可保证 SIS 不受危险影响应使用的规程。

a) 现场传感器

BPCS 和 SIS 共用一个传感器时要求进一步地复审和分析。因为此单一传感器的失效可能产生一种危险情况,故有必要进行额外的复审和分析。例如:当 BPCS 和 SIS 使用同一个液位传感器,传感器低位失效时,高液位脱扣会产生一次要求。传感器低位失效导致控制器将驱动阀门开启,由于 SIS 也使用该传感器,而它并不会检测到作为结果而产生的高液位工况。

在一个 BPCS 和 SIS 功能使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的要求。

实际上,即使是在 SIL 1 应用的情况,也难以达到这一点。对一个 SIL 2、SIL 3 或 SIL 4 的仪表安全功能来说,通常需用具有同型或异型冗余的单独 SIS 传感器来满足要求的安全完整性。

注 2:当使用一个单独 SIS 传感器时,通过适当的隔离器把信号转发给 BPCS 是有好处的。通过对 BPCS 和 SIS 传感器之间的信号进行比较,这种安排可能提高诊断覆盖率。

当使用冗余 SIS 传感器时,通过适当的隔离器也可把这些传感器连接到 BPCS 上。BPCS 中的适当算法,通过降低对 SIS 的要求率,如"取中间值(middle of three)",可提高安全性。

b) 最终元件

BPCS 和 SIS 共用一个阀门的情况大致同共用一个传感器的情况一样,也需要进一步地复审和分析。如果阀门失效将向 SIS 提出一次要求,通常不推荐 SIS 和 BPCS 共用一个阀门。

在 BPCS 和 SIS 只使用一个阀门的情况下,一般仅当阀门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的要求。

实际上,即使对 SIL 1 应用而言,要达到上述要求也是困难的。对一个 SIL 2、SIL 3 或 SIL 4 仪表安全功能而言,要满足安全完整性通常需要 SIS 具有同型或异型冗余的单独阀门。

在 BPCS 和 SIS 功能使用单一阀门的情况下,设计应保证 SIS 动作超驰(overrides)BPCS 动作。一般可通过把 SIS 直接连接到一个电磁阀上来达到这个要求,该电磁阀可直接断开执

行器的动力源，例如在阀门定位器和执行器之间。

当使用冗余 SIS 阀门时，这些阀门可同时连接到 SIS 和 BPCS 上。

注 3：即使使用冗余阀门，考虑 BPCS 阀门和 SIS 阀门之间的共同原因失效也是重要的。

确定阀门要求的附加考虑有：

——截断要求；

——类似过程应用中阀门可靠性的经验；

——阀门的非安全失效模式；

——降低阀门作用的操作规程(例如开启旁路阀门)；

——检验测试要求。

c) 配线

有关给脱扣系统供电的问题，通常 BPCS 和有关现场装置的配线是同 SIS 和它的现场装置的配线分开的，这是因为安全功能可能意外失效而不通知脱扣系统。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，建议使用良好的标号和维护规程。

注：给脱扣系统供电涉及到 SIF 电路，在正常工作状态下，该电路的输出和装置处于断电状态下。施加动力(如电、气体)就产生一次脱扣动作。

加电脱扣系统和断电脱扣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。关于给脱扣系统供电的问题，可附加对火灾风险区电缆支架防火的考虑。

11.2.5 见GB/T 21109.1。

11.2.6 有关的指南和GB/T 21109.1—2007的 11.2.5 的注应遵循的指南见本部分的 11.8。

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，人的效能也是系统设计的一个元素。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)应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 Guideline for Improved Human Performance in Process Safety, New York: American Institute of Chemical Engineers (1994)。

CCPS/AIChE Guideline for Chemical Process Quantitative Risk Analysis (second edition), New York: American Institute of Chemical Engineers (2000)。

HSE Reducing error and influencing behaviour, HSG48, Health and Safety Executive, London (1999), ISBN 07176 2452 8。

11.2.7 本条论述了如果在纠正脱扣工况后，SIS 立即自动重新起动该过程时可能产生的潜在危险。应分析每个 SIF，以便确定一旦纠正了脱扣工况应怎样复原该 SIF。一般应只有在操作员的手动动作之后，才可能重新起动。

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机。在 SRS 中通常定义有手动停机的要求。

倘若必要并且危险和风险评估组认为合适，就可把紧急停机连接到 SIS PE 逻辑解算器(例如当要求按顺序停机时)。

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—2007的图 9)。

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，在这种情况下必须按照GB/T 21109.1实现共用或共享设备。

在共用设备的失效可引起向 SIS 提出一次要求的情况下，应进行一次分析以保证总危险率满足预期值。总危险率是所有共用元素的危险失效率和其他要求源的危险率(包括 SIS 的各个独立部分的危险失效)的总和。为了确定与共用设备的危险失效相关的危险，应考虑以下情况：

a) 冗余配置的一个元素被用作一个 BPCS 的情况。考虑仪表故障引起的 SIS 性能降低时共用设备的危险失效产生的危险。

b) 共享仪表非冗余的情况。考虑假定 SIS 不会响应时共用设备的危险失效导致的危险。

11.2.10 提供 BPCS 和 SIS 二者所使用的一个共用元素的注意指南。注中的“足够低”意味着由其他独立层(不是 SIF)的 PFD 组合成的共享设备的危险失效率仍满足你的共同风险准则。

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(例如给脱扣系统供电)的情况下，应考虑包含本地手动方式达到安全状态的条款。

11.3 检测故障时的系统行为要求

11.3.1 见GB/T 21109.1。

11.3.2 见GB/T 21109.1。

11.3.3 见GB/T 21109.1。

11.4 硬件故障裕度要求

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。

本部分认识到过程工业中安全系统的性能不只需要一级，因此本部分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所涉及的特殊应用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，本部分要求执行一次可靠性分析。

本部分的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，应考虑以下一系列因数：

——在子系统中使用的装置的复杂程度。如果已很好定义了故障模式并能确定故障工况下的行为以及有足够的来自现场经验的失效数据，则一台装置不大可能发生系统故障。

——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，这种能力被称为装置的安全失效分数。

——应用所涉及的安全完整性等级要求。

制定GB/T 20438—2006的工作组考虑到了上述因素以及在GB/T 20438.2—2006中要求规定的故障裕度值。在拟制过程部门的该部门专用标准时，应考虑到现场装置和非 PE 逻辑解算器的故障裕度要求可被简化，并且GB/T 21109.1可作为替代标准。应注意，为了满足可用性要求，子系统设计可能要求比GB/T 21109.1—2007的表 5 和表 6 中所讲的部件冗余更大。

硬件故障裕度要求可适用于执行某个 SIF 所需的各个部件或者子系统。例如，在包含有若干个冗余传感器的一个传感器子系统的情况中，故障裕度要求适用于整个传感器子系统，而不适用于各个传

感器。

11.4.2 GB/T 21109.1—2007的表5定义了PE逻辑解算器的最低故障裕度。故障裕度要求依赖于SIS所要求的SIL以及子系统安全失效分数。通常可从PE逻辑解算器供货商处得到逻辑解算器安全失效分数的有关信息。如果未按照计算安全失效分数时所作的假设来使用PE逻辑解算器,则应仔细考虑对安全失效分数所作的声明。特别是应检查所作的假设,以保证在计算SFF时所假定的边界和环境对现实应用是有效的。这是因为SFF同许多问题有关,比如子系统是加电脱扣还是断电脱扣。在计算SFF过程中所使用的数据源和所做的假设都应文档化。SFF只同硬件随机失效有关。在确定SFF时,以下假设是可以接受的,即应用所选择的子系统是恰当的,并且子系统的安装、调试、运行和维护都准确无误以至可以在评估中忽略掉早期失效和老化失效。在确定SFF时无需考虑人为因素。

11.4.3 GB/T 21109.1—2007的表6定义了具有第1列中所要求的SIL声明限值的传感器、最终元件和非PE逻辑解算器的基本故障裕度水平。表6中的要求是以GB/T 20438.2—2006中对具有SFF在60%～90%之间的PE装置的要求为依据的。这些要求所依据的假设是主导失效模式将进入某个安全状态或者危险失效已被检测出。

11.4.4 本条允许除PE逻辑解算器外的所有子系统的硬件故障裕度在某些条件下可减少1。这些条件适用于包括阀门或者智能变送器等装置,并可降低系统失效的可能性,从而使对非PE装置的要求同GB/T 20438.2—2006的要求相一致。

11.4.5 在某些情况下按照GB/T 20438.2—2006的故障裕度要求有可能降低故障裕度。它可以通过引入附加诊断(如信号比较或定期进行的部分行程测试)来实现,从而使子系统的SFF高于90%。

11.5 选择部件和子系统的要求

11.5.1 目的

见GB/T 21109.1。

11.5.2 一般要求

11.5.2.1 选择SIS中使用的部件和子系统时有一些考虑。首选是按GB/T 20438.2—2006和GB/T 20438.3—2006设计的部件。第二选择是使用在类似服务和类似环境中经广泛使用已知是可靠的部件和子系统。

无论选择那个选项,都应论证部件或子系统:

a) 充分可靠足以达到总的目标PFD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。

只要符合GB/T 20438.2—2006和GB/T 20438.3—2006或者本部分的11.5中以往使用的要求就能满足c)的要求。

11.5.2.2 见GB/T 21109.1。

11.5.2.3 见GB/T 21109.1。

11.5.2.4 见GB/T 21109.1。

11.5.3 根据以往使用选择部件和子系统的要求。

11.5.3.1 只有少数现场装置(传感器和阀门)是按照GB/T 20438.2—2006和GB/T 20438.3—2006进行设计的。因此,用户和设计人员不得不更依赖于使用"经使用验证的"现场装置。

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。这些清单是根据它们的BPCS的广泛成功操作经验而创建的。那些执行情况不理想的传感器和阀门被剔除在清单之外。

按照GB/T 21109.1的要求对SIS进行评估时,通常BPCS的认可或推荐清单上所列的传感器和阀门也可认为是经使用验证的。此仪表清单应包含装置的版本,并得到从用户和制造商反馈的现场监视的文档的支持。此外,制造商应有一个修改过程,以评价已报告的失效和修改的影响。

如果没有这样一份清单,用户和设计人员就需要对传感器和阀门进行一次评估,以保证它们能确信

仪表将按要求执行。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。

11.5.3.2 应注意到对一些比较复杂的装置而言,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,现场装置操作行规的相关特征与逻辑解算器操作行规的相关特征是不同的。

对现场装置而言,以下几点应成为操作行规的组成部分:

——功能性(如测量、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,以下几点应成为操作行规组成部分:

——硬件版本和结构;

——系统软件版本和组态;

——应用软件;

——I/O 组态;

——响应时间;

——过程要求率。

对所有装置而言,以下两点应成为操作行规的组成部分:

——EMC;

——环境条件。

11.5.4 根据以往使用选择 FPL 可编程部件和子系统(如现场装置)的要求。

11.5.4.1 见GB/T 21109.1。

11.5.4.2 见GB/T 21109.1。

11.5.4.3 见GB/T 21109.1。

11.5.4.4 本条说明鉴定一个 FPL 可编程装置是否具备 SIL 3 能力时的附加要求。

11.5.4.5 本条强制要求一个具有 SIL 3 能力的 FPL 可编程装置必须具备一本安全手册。

11.5.5 根据以往使用选择 LVL 可编程部件和子系统(如逻辑解算器)的要求。

11.5.5.1 本条列出了对具有 SIL 1 或 SIL 2 能力的 LVL PE 逻辑解算器的附加要求。具有 SIL 3 或 SIL 4 能力的 LVL PE 逻辑解算器应符合GB/T 20438.2—2006和GB/T 20438.3—2006。

11.5.5.2 见GB/T 21109.1。

11.5.5.3 见GB/T 21109.1。

11.5.5.4 见GB/T 21109.1。

11.5.5.5 本条列出了一个安全配置的 PE 逻辑解算器要达到 SIL 1 和 SIL 2 能力的附加要求。有关附加考虑可参见附录 D。

11.5.5.6 本条列出了一个安全配置的 PE 逻辑解算器要达到 SIL 2 能力的附加要求。

11.5.5.7 本条强制要求一个具有 SIL 2 能力的 LVL 可编程装置必须具备一本安全手册。

11.5.6 选择 FVL 可编程部件和子系统(如逻辑解算器)的要求。

11.5.6.1 见GB/T 21109.1。

11.6 现场装置

11.6.1 见GB/T 21109.1。

11.6.2 见GB/T 21109.1。

11.6.3 见GB/T 21109.1。

11.6.4 见GB/T 21109.1。

11.7 接口

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仪表安全功能的组成部分,则应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,停机开关(实现停机动作的方式)应被认为是SIF的一部分。

如果能表明并不包含仪表安全功能(如BPCS中的只读访问),则可在BPCS中显示非SIF组成部分的数据通信(例如,实现SIF中的脱扣功能时,可显示一个SIF传感器的实际值)。

11.7.1 操作员接口要求

在操作员和SIS之间用于交流信息的操作员接口可包括:

——视频显示器;

——包含灯、按钮和开关的面板;

——声光报警器(可视和可听);

——打印机(不应是通信的惟一方法);

——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,应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有关的视频显示应能清晰地识别,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仪表安全功能和BPCS报警功能的自动事件记录。

应记录的工况可包含:

——SIS事件(比如脱扣和并发预脱扣);

——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

面板应安放在操作员容易达到的地方。

面板上的布置应保证按钮、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机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况的操作员可能停错设备。因此各停机开关应在形体上加以区分,并应标记好各自的功能。应提供测试所有灯的方法。

c) 打印机和记录

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,不应危及仪表安全功能。

利用时间和日期标记以及工位号标识,打印机可用来记录事件发生的时序、诊断、其他事件和报警。应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),则应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。

11.7.1.1 应在一个显示器上向操作员提供足够的信息,以便迅速传送关键信息。显示器的一致性是重要的,所使用的方法、报警约定和显示部件应同 BPCS 显示器一致。

还应注意显示器布置。应避免在一个显示器上安排大量信息,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应被用于指引操作员到重要信息上,从而减少混淆的可能性。信息应清楚、简明扼要和无歧义。

显示器设计应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。

11.7.1.2 见GB/T 21109.1。

11.7.1.3 见GB/T 21109.1。

11.7.1.4 见GB/T 21109.1。

11.7.1.5 见GB/T 21109.1。

11.7.2 维护/工程接口要求

11.7.2.1 见GB/T 21109.1。

11.7.2.2 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装置:

a) 系统硬件配置;

b) 应用软件开发、文档编制和下载到 SIS 逻辑解算器;

c) 为了更改、测试和监视而对应用软件进行的访问;

d) 查看 SIS 系统资源和诊断信息;

e) 更改 SIS 保密等级以及存取应用软件变量。

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

维护/工程应提供把应用程序复制到备用存储媒体上去的一些手段。

与一个 SIS 连接的、用于维护/工程目的的个人计算机在出现故障、掉电或断开连接时应不危及安全功能。

11.7.2.3 见GB/T 21109.1。

11.7.2.4 见GB/T 21109.1。

11.7.3 通信接口要求

11.7.3.1 见GB/T 21109.1。

11.7.3.2 见GB/T 21109.1。

11.7.3.3 见GB/T 21109.1。

11.7.3.4 见GB/T 21109.1。

11.8 维护或测试设计要求

11.8.1 设计 SIS 应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,设计不应要求断开线路、使用跳线或者强制软件寄存器,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,系统设计应提供 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,则需提供有关在保持过程安全的同时维护部门应怎样处理这些仪表而又不会引起一次乱真脱扣的考虑。

对最终元件测试周期的任何限制都应在计算 SIF 的 PFD_{avg} 时加以考虑。

11.8.2 见GB/T 21109.1。

11.8.3 安装旁路可能降低一个 SIS 的保密水平。通过以下办法可以克服保密性的这种降低：

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。

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，应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，设计应尽量使 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。

11.8.4 见GB/T 21109.1。

11.9 SIF 的失效概率

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，用户和设计人员应参见本部分的附录 A。

11.9.2 本部分附录 A 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。GB/T 20438.2—2006的 7.4.4.5 和 7.4.4.6 条提供了怎样确定诊断的要求(有关怎样计算诊断覆盖率的例子另见GB/T 20438.6—2006的附录 C)。

提高 SIS 的诊断覆盖率有助于满足 SIL 要求。在这种情况中，当计算 SIS 的失效概率(要求模式)或者失效频率(连续模式)时，应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 20438.6—2006的附录 B 或者 ISA TR84.00.02。

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 中的故障，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应小于“过程安全时间”。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。

共用部件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，应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应满足安全要求规范。

在这些诊断程序并不是“内装”在厂家提供的设备中时，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(比如软件误差)。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，它们包括：

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装置。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变送器的高温脱扣应用中，可附加一个超下限报警器来诊断变送器失效或者变送器信号丢失。

2) 如果使用冗余变送器，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 个变送器，可使用 3 个读数的中间值(中值选择)。因为不能正确执行功能

的装置会使平均值跑偏，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：

——脉冲导管中的闭塞或冷凝；

——吹洗源压力的降低；

——热电偶覆盖层；

——接地或电源问题；

——变送器不响应，其输出值始终不变。

3) 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乱真报警，可提供时间延迟。例如，有的冗余流量传感器有1 s～2 s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。

4) 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，从而验证已经采取了预定动作。应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。只是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

安全专用的或者符合GB/T 20438—2006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(程序)。

关于可靠性数据的置信度可参见GB/T 21109.1—2007的11.9.2 c)中的注，平均无故障时间(MTTF)典型地可通过记录在累计运行时间(T)内，在一个部件样本中发生的失效数(n)确定。使用“Chi-square”测试(参见“可靠性、维修性和风险，D J Smith” ISBN 0 7506 5168 7)可推导出所得到的MTTF的置信度水平。这意味着通常在一个SIS的可靠性计算中应使用的MTTF值要比由T/n计算的MTTF值低。要求的置信度水平越高和观察到的失效数据越低，降低系数也就越大。但一般来说，合理的假定为：置信度水平为70%时，同可靠性建模相关的其他不确定源相比，降低系数不显著。

12 应用软件要求，包括工具软件的选择准则

GB/T 21109.1—2007的第12章并不对SIL 3和较低SIL的应用软件设计方法加以区别，因为经验表明当使用以下工具时，两种方法之间的差别不大：

——FPL或LVL；

——符合GB/T 21109.1的逻辑解算器；

——相应的安全手册。

对不同SIL的测试和验证可能会有差异。这方面的指南可参见本部分的12.7.2.3。

12.1 应用软件安全生命周期要求

12.1.1 目的

12.1.1.1 见GB/T 21109.1。

12.1.2 要求

12.1.2.1 见GB/T 21109.1。

12.1.2.2 注1和注2：当应用软件的设计、实现、验证和确认使用有限可变语言，比如GB/T 15969.3

中的梯形图或者功能块图时，则只需应用图3中所示标准软件“V”模型的两层。在这种情况下，假定使用的功能块符合GB/T 20438.3—2006，则：

——在某种程度上，每个SIF的软件使用“应用软件结构设计”可保证软件设计同硬件结构相一致；

——“应用软件开发”被解释为使用符合GB/T 20438.3—2006和GB/T 20438.4—2006的有限可变语言的安全逻辑的设计和实现；

——“应用软件测试”被解释为应用软件的验证和测试；

——“应用软件同SIS子系统的集成”被解释为使用有限可变语言实现的每个过程安全功能的集成和验证。

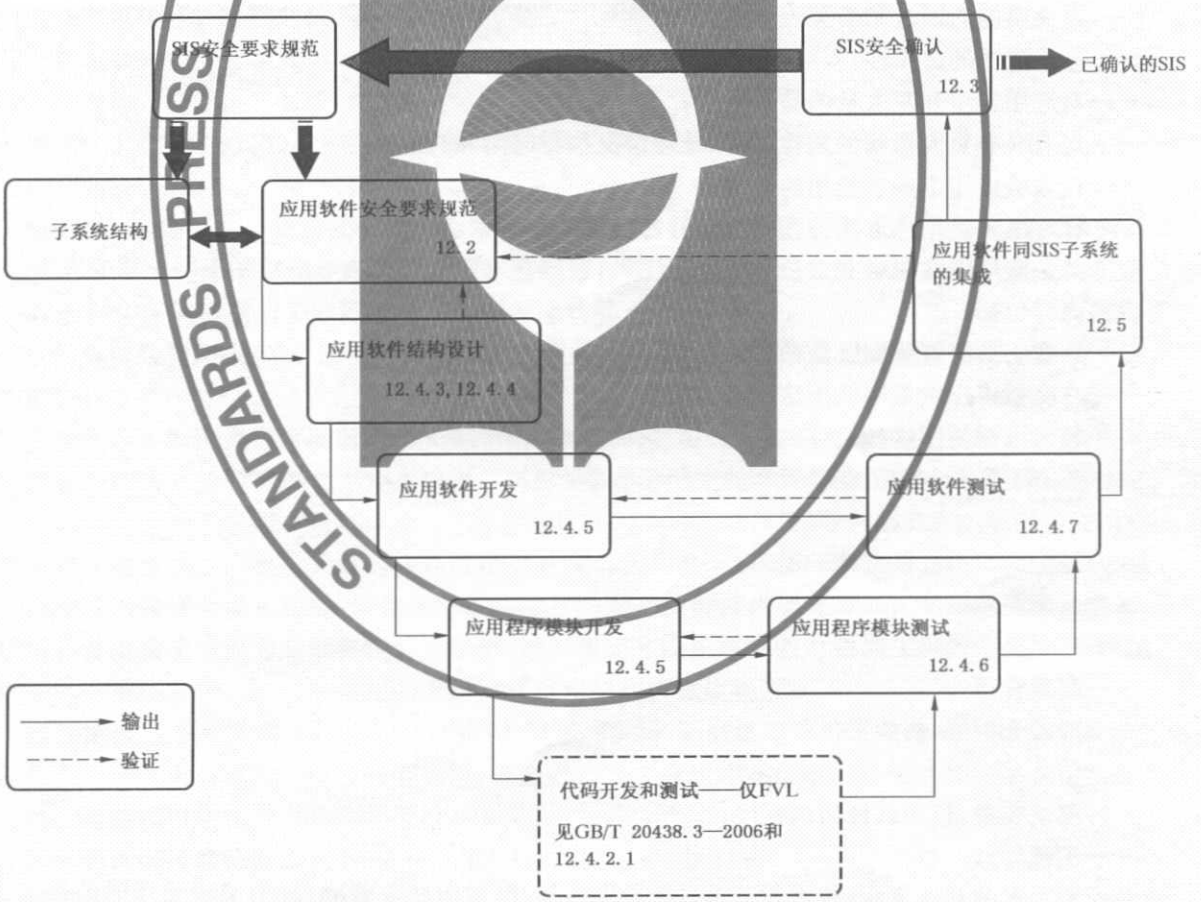
在附录D中给出了使用符合GB/T 20438—2006 SIL 3的一个PLC的应用软件开发生命周期的例子。

在使用符合GB/T 20438—2006的有限可变语言元素来实现一个新的“功能”或者“功能块”的情况下（例如通用燃烧器联锁序列或者泵联锁序列），则：

——“V”模型中的“应用程序模块开发”被解释成新功能的设计和实现；

——“应用程序模块测试”被解释成新功能的验证和测试。

在用全可变语言编写一个新功能，并因此需要开发软件代码的情况下，正如“V”模型（图3）指出的那样，开发者应遵守GB/T 20438.3—2006所定义的所有生命周期阶段和规程。



注：除非另有说明，本图中的条文号指的是GB/T 21109.1中的条文号。

图3 软件开发生命周期（V模型）

12.1.2.3 见GB/T 21109.1。

12.1.2.4 选择方法、技术和工具的一些考虑：

为了选择有助于软件达到所要求的质量的方法、技术和工具，应考虑应用软件的下列关键质量

参数：

——简明性；

——合适的注释和自然语言的支持；

——用于反映应用的分类法；

——测试覆盖率；

——在支持过程中所涉及到的人员的易理解性；

——与其他相关应用软件风格的通用性。

识别重要参数的方法包括：

——同风险承担者进行讨论，包括操作和维护；

——复审当前作法和工业标准；

——复审厂商的建议；

——分析早先的经验；

——与同行进行讨论。

为使重要的质量参数最佳，在选择方法、技术和工具时应考虑以下问题。

在开发过程中，所选择的方法、技术和工具应使在应用软件中引入故障的风险降到最低。应考虑的内容包括：

——定义明确的语法和语义；

——应用程序的适用性；

——对应用程序开发人员的易理解性；

——对 SIF 有重大影响的属性(例如最坏情况执行时间)的保证；

——在类似应用中成功使用的证据；

——针对限制使用该方法的“非安全”特性的规则和约束。

应选择一些用于实现这些方法和技术的工具，以便在这些方法和技术的实际应用中减少人为误差。应考虑的内容包括：

——这些工具应被开发团队的相关成员所熟悉；

——在类似应用中成功使用这些工具的证据；

——针对限制使用这些工具的“非安全”特性的规则和约束；

——所有工具和 SIS 的准确版本的文档化清单；

——不同工具之间以及不同工具和 SIS 之间的可兼容性；

——可生成应用软件文档的能力。

在生命周期阶段使用的工具的典型例子包括：

——应用程序代码生成器；

——配置管理；

——静态分析器(例如工位名检查程序、扫描时间检查程序)；

——仿真器；

——测试装置，包括软件测试程序；

——工程师站。

还应考虑到的其他方法、技术和工具包括尺度测量(例如测试覆盖率)和为了增强功能的验证而使用的不同的工具(例如背对背工具)。

为了发现并消除软件中已有的故障，建议在整个开发生命周期各阶段都进行验证。典型的方法在12.7.2.3中描述。

为了确保软件中残留的故障不会导致不可接受的后果，需考虑：

——在线检查技术和异常处理；

——供方场外数据库和全局故障报告的使用；
——SIS 故障报告和过程问题及它们对 SIS 的影响的监视；
——在其他系统中对 SIS 关键功能性的镜像；
——在培训过程中 SIS 应用软件副本的使用。

为了保证能在整个 SIS 生存期进行软件维护，需考虑以下几项：

——更改管理的程序(见GB/T 21109.1—2007的第 17 章)；
——进行中的管理支持和维护培训；
——在整个 SIS 生存期中支持工具和开发平台的可用性；
——促进足够的人力资源和技术贯穿 SIS 整个生命周期的方法，这些方法是成文并适宜被广泛使用的；
——针对便于理解和限制软件更改的影响的开发和文档编制规则的使用；
——“初建的”和最新的文档集；
——开发能力和离线测试能力。

12.1.2.5 见GB/T 21109.1。

12.1.2.6 见GB/T 21109.1。

12.1.2.7 见GB/T 21109.1。

12.1.2.8 见GB/T 21109.1。

12.2 应用软件安全要求规范

12.2.1 目的

12.2.1.1 见GB/T 21109.1。

12.2.2 要求

SIS 整体结构也许给规定的仪表安全功能加了一些额外的功能软件要求。一个典型的示例就是冗余传感器的 1oo2 选择逻辑，以及通过传感器自诊断检测到一次危险失效时采取的一个规定的安全动作。附录 B 中的例子列出了来源于所用结构的那些要求。

应用软件也应考虑 PES 所提供的诊断。开发应用软件是为了采取逻辑解算器安全手册中定义的适当动作。

一般使用逻辑图或因果图就可定义每个仪表安全功能的详细安全要求。在许多情况下，可使用逻辑解算器厂家提供的编程语言来定义要求。可以使用的典型语言有功能块图或因果矩阵。所选的厂家提供的语言应适合于应用。使用厂家提供的语言来定义详细要求常常可避免从其他形式的文档翻译成要求时发生的错误。应提供大量的注释以便定义安全和非安全功能以及所有安全功能的 SIL 要求。

详细的功能安全要求规范，应包含受保护过程的所有操作模式期间的所有必要的功能。此外，还应提供所有仪表安全功能的定期测试。典型地，这要求定义维护超驰能力，以便在不停止过程的情况下测试传感器和最终元件。上段中描述的方法同样可用来文档化这些要求。

当使用多个 SIS 来实现仪表安全功能时，应提供用来说明在每个 SIS 中应实现哪些功能的文档。如使用多个 SIS 来实现同一仪表安全功能，则应把 SIS 之间的相互作用以及每个 SIS 的独立性文档化。该文档应包括预定的每个 SIS 应提供的 SIL。

另外的指南可参见本部分的 10.2.1 和 10.3.1。

12.2.2.1 见GB/T 21109.1。

12.2.2.2 在开发应用软件之前，用户应提供一份过程风险和危险评估，根据仪表安全功能以及它们的 SIL，此评估可用来确定软件安全要求。一旦做出了实现软件中仪表安全功能的决定，就应处理好安全要求规范中的任何冲突、不一致和遗漏，这些都是软件设计师需要注意的。一个例子可以是软件内仪表安全功能执行次序的影响。另一个例子是当应用软件与能源关断有关时，应用软件的响应。

12.2.2.3 应用软件安全要求应被作为 SIF 安全要求规范的一个可追溯的响应来开发，涉及的要素

包括：

——实现用户定义的 SIF 所需的功能性和定时要求；

——软件系统与过程和人的接口；

——过程危险和应用软件提供的功能性之间的关系；

——保持在过程安全包之内所允许的应用软件的行为边界(例如，处理误差的输入条件的排除)；

——逻辑解算器中提供的实用软件的允许的功能性(例如，安全逻辑和 I/O 通信，故障处理和系统诊断之间的优先次序区分)；

——应用软件执行的硬件平台和系统软件以及硬件和系统软件的配置；

——在过程中，由于系统(软件是该系统的一部分)功能性所产生的危险(例如，断电时不适当的硬件失效模式)；

——作为支持逻辑解算器安全手册时，设计师所使用方法和规程的约束。

为了避免在开发过程的较晚阶段出现困难，制定用于表明已达到应用软件要求的策略也很重要。

在应用软件用于安全仪表系统的情况下，功能安全评估可包括：

——用于表明应用软件功能达到过程危险要求的检查技术；

——用于表明应用软件已执行过所要求的功能，而且到目前为止软件中任何额外的功能不会导致危险工况的功能测试；

——用于表明应用软件在指定的时间已执行所要求的功能的结构测试；

——用于表明应用软件不会产生危险工况的功能失效分析，以及“如果…就会怎样”(“what if”)分析；

——用于表明开发和验证的受控过程已到位，并且使用正确软件版本的审核。

12.2.2.4 见GB/T 21109.1。

12.2.2.5 见GB/T 21109.1。

12.2.2.6 见GB/T 21109.1。

12.3 应用软件安全确认计划编制

附加的指南可见 10.3。

12.3.1 目的

12.3.2 要求

12.3.2.1 见GB/T 21109.1。

12.4 应用软件设计和开发

12.4.1 目的

12.4.1.1 见GB/T 21109.1。

12.4.1.2 见GB/T 21109.1。

12.4.1.3 见GB/T 21109.1。

12.4.1.4 见GB/T 21109.1。

12.4.1.5 见GB/T 21109.1。

12.4.2 一般要求

有许多用来提供 SIS 中安全应用软件的方法。然而，不管使用什么方法来实现安全应用软件，都需要保证已经正确执行完安全生命周期中开发应用软件之前的所有步骤(例如，危险和风险评估、功能描述编写、设备(硬件和软件)选择)。

在设施还没有经验、支持或故障排除能力时，在实现下面的方法之前，建议进行培训和积累操作经验(最好是在非安全应用中的经验)。为了增强此工作，设计和开发人员应建立与在同样环境下使用同样设备的 PE 逻辑解算器用户之间的联络。此办法的置信度水平是确定在 SIS 应用中使用 PE 逻辑解算器的一个主要因素。

下面是开发 SIS 应用软件时需考虑的一个项目清单：

——把应用软件分解成一些离散的 SIF，使每个 SIF 都具备一个 SIL；

——弄清楚每个 SIF 的硬件结构并在每个 SIF 的应用软件中复制此硬件；

——如果优化应用软件过于复杂，则不要优化(常需要一位高级程序员来解释应用软件)；

——根据厂家说明书(例如安全手册)，使用应用软件开发技术；

——不能把从一个 SIF 中得到的应用软件同其他任何一个 SIF 组合起来；

——在经过培训，能够理解和排除故障的基础上使用应用软件语言(如类型、功能)；

——提供一份写好的应用软件描述，该描述同功能描述是一致的，并同应用软件文档放在一起；

——根据过程流程对应用软件进行模块化(例如，第一个模块是与 SIF 无关的通用应用软件，但它是 SIS 所必需的，第二个模块是位于过程入口处的第一个 SIF，最后一个模块是位于过程出口处的最后一个 SIF)；

——充分测试(如仿真、检查、复审)每个应用软件模块并得到第二次独立分析(包括此时的操作和维护部门以及在所有的后续步骤中)，充分测试构成一个过程子系统的模块组合并得到第二次独立分析；

——充分测试 SIS 应用软件；

——获得第二次独立分析；

——在检验完硬件后(例如证实 I/O 已连接到正确的传感器/最终元件上)，使用应用软件；

——包括在过程试运行(如过程不加危险材料运行)中测试应用软件；

——当过程流转到设施时(例如调试运行)，应用软件支持小组成员应守在现场。

应用软件文档可用来确定应用软件对每个 SIF SIL 的适用性。应进行独立的分析来确定应用软件满足 SIL 等级。

GB/T 20438.3—2006和GB/T 20438.6—2006提供了关于此问题的一些替代方法和进一步指南。

12.4.2.1 见GB/T 21109.1。

12.4.2.2 关于选择应用软件设计方法和技术的指南，安全要求达到 SIL 3 的系统应按供货商的安全手册中给出的说明来设计，作为符合GB/T 20438—2006系统的一部分。对于 SIL 4 的系统而言，开发者还应证实所选方法的确符合GB/T 20438.3—2006的要求。

关于选择应用软件测试和验证方法及技术的问题，根据 12.7 中给出的指南来验证安全要求达到 SIL 3 的系统。对于 SIL 4 的系统，验证人员还要证实所选方法的确符合GB/T 20438.3—2006的要求。

12.4.2.3 见GB/T 21109.1。

12.4.2.4 为了保证可测试性，通常建议在设计和开发阶段就考虑应用软件的集成测试规范。

12.4.2.5 在一个 SIS 中应用软件要实现不同 SIL 的仪表安全功能时，应把实现这些功能的软件清楚地分开并作好标记。这使得每个仪表安全功能的软件都能追溯到正确的传感器和最终元件冗余，也使得功能性测试和功能的验证测试与 SIL 相匹配。标签应标明 SIF 和 SIL。

软件的分离区域可用于非仪表安全功能和仪表安全功能。证明充分独立的一种方法要遵从：

a) 应用软件中的仪表安全功能被清楚地标记成 SIF 应用程序代码；

b) 应用软件中的非仪表安全功能被清楚地隔离；

c) 在实现仪表安全功能时使用的所有变量都被标记；

d) 实现非仪表安全功能的所有应用程序码都被标记成非仪表安全功能代码；

e) 使用非安全变量和 SIF 变量的所有应用程序代码满足以下条件：

——非安全应用程序代码(程序、功能和功能块)不写入安全应用程序代码中使用的任何 SIF 变量；

——在实现仪表安全功能时，安全应用程序代码与任何非安全变量无关。

f) 所有安全应用软件(即代码和变量)都被保护，以防任何非安全软件更改；

g) 如果安全和非安全软件共享同样的资源(例如 CPU、操作系统资源、存储器、总线),则绝不能危及安全应用软件的仪表安全功能(例如响应时间)。

理想的情况下,应用程序开发软件应自动检验应用程序代码(SIF 和非安全功能)和所有变量(SIF 和非安全功能)之间的交互。如果不能提供此性能,应用软件开发者、执行验证和确认应用软件的其他人员应检验所有的应用程序代码和相关变量以与上面所给出的分离规则相一致。

12.4.2.6 见GB/T 21109.1。

12.4.2.7 见GB/T 21109.1。

12.4.3 **应用软件结构要求**

在一个典型的 SIS 逻辑解算器中,软件结构可能的变化是很有限的,并可通过观察应用程序开发的主要步骤最深刻地理解这些变化。在开发和测试应用程序中,通常开发者需执行下列主要步骤:

a) 配置 I/O 模块和内存变量数据区。

b) 编制所有 I/O 和内存变量的工位名。工位命名应遵循一致的约定。

c) 定义维护超驰技术。有些用户要求用数字输入开关替代硬接线开关启动维护超驰。另外一些用户则要求使用来自一个显示站的受控数据输入到 SIS 中。在任何一种情况下,一定要确保安全处理从而避免意外的超驰。应通报维护超驰。

d) 定义传感器和最终元件诊断以及定期测试的基本原则。这与传感器和最终元件的冗余有关。需对基本原则进行仔细定义,而且其中应包含测试期间合适的报警。

e) 定义与 SIS 相连的其他外围系统的通信变量。如果这些变量是内存变量,一定要把它们分配给适当的数据区以便通信子系统能对它们进行存取。应仔细定义能被 SIS 的其他外围系统修改的这些变量,通常情况下这些变量被存放在存储器的特殊读/写区。

f) 定义事件序列记录在什么地方和怎样记录事件序列,并了解这些事件对 SIS 的影响。

g) 开发定制的功能和功能块。由于在应用程序中可对重复性操作进行编程、重复测试和使用,所以这种定制是非常必要的。

注:在GB/T 15969.3中定义了功能、功能块和程序。

h) 确定一个给定程序中应包含哪些仪表安全功能和其他功能。有必要把安全功能和非安全功能分离存放在独立的程序中,从而把着重点放在安全关键程序上。也要求限制一些功能的程序大小。

i) 开发应用程序。应用程序结构应同过程结构一致(例如,在一个化工厂中,应把每个过程单元的应用程序分到一组。在每个过程单元范围内,为了便于了解和维护,设备之间应相互隔离)。

j) 确定每个程序内网络和逻辑的正确执行顺序,以及所有应用程序的执行顺序和要求的执行速率。确保应用程序的执行速率同软件安全要求规范所要求的过程响应时间一致。

k) 使用开发环境的监视能力(在可用的情况下)测试应用软件。

l) 把应用软件下载到逻辑解算器中。

m) 测试所有逻辑解算器输入、输出、应用软件和同 SIS 相连的其他外围系统的接口。

12.4.3.1 见GB/T 21109.1。

12.4.3.2 见GB/T 21109.1。

12.4.3.3 见GB/T 21109.1。

12.4.3.4 见GB/T 21109.1。

12.4.3.5 安全数据完整性验证的例子包括:

——超出范围的 I/O 数据的检验;

——通信的应用数据的确认;

——工位命名的一致性检查,例如重复使用同一工位名的检查;

——超驰有效性检验,例如维护和启动超驰有效性检验;

——报警和设定点的有效性检验。

12.4.4 支持工具、用户手册和应用程序语言的要求

开发环境是一组支持应用软件编码、应用程序参数和接口的配置以及应用软件执行的测试/监视的工具。通常情况下开发环境可提供以下功能：

a) 配置编辑器。此编辑器用来配置I/O子系统、I/O内存变量和通信功能。

b) 语言编辑器。应用程序员可用这些编辑器开发执行系统所需的全部功能(安全和非安全)的程序。

c) 经认证的功能和功能块库。这些功能和功能块可用于应用程序中。

d) 定制功能和功能块开发能力。有些供应商提供一个开发环境，使用户能开发被支持的应用程序语言所使用的定制功能和功能块。在用于应用程序之前，应充分测试这些功能和功能块。

e) 应用程序调度工具。这些调度工具支持对所要求执行序列的次序及执行程序序列的扫描速率所进行的设置。

f) 下载能力。它使开发者能把应用程序、功能块库、可变数据和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。有的供应商提供具有在支持开发环境的计算机上仿真所有应用程序能力的开发环境，那么就能在把应用程序下载到逻辑解算器中之前，对应用程序进行充分地离线测试。

h) 程序监视能力。监视能力可使用户在用户定义的屏幕上或者在实际的功能块屏幕上或者梯形图程序屏幕上观看到来自执行程序的数据。开发环境还提供了监视仿真程序执行的功能。此外，也能监视逻辑解算器中程序的执行。

i) 逻辑解算器的诊断显示器。这些显示器可显示系统中主处理器模块、通信模块和I/O模块的状况。通常情况下可显示每个模块的合格、不合格(有故障)、激活状况；在许多情况下，也可提供关于系统中故障的详细信息。

12.4.4.1 见GB/T 21109.1。

12.4.4.2 见GB/T 21109.1。

12.4.4.3 见GB/T 21109.1。

12.4.4.4 建议所使用的应用程序语言编译器最好是检验过的和/或通过认可的工业标准认证过的。

12.4.4.5 见GB/T 21109.1。

12.4.4.6 见GB/T 21109.1。

12.4.4.7 安全手册示例

在符合本部分的SIF应用中使用的部件和装置应提供描述安装、维护、配置、编程和操作的所有已知细节的文档以表明部件或装置是否满足应用的安全要求规范。

本部分常被称为部件或装置的“安全手册”。然而，它可由供货商安装、维护标准以及包含一个附加文档的用户手册组成，该附加文档规定了它在SIF应用中使用、在这些应用中使用的限制、在诊断报警时和已知失效模式下应采取的动作等有关方面的问题。“安全手册”还应定义在一个SIF应用中使用部件或装置时不应使用的特征、配置和/或程序语句类型。

有限可变编程允许使用全局数据；因此，安全手册应指导程序员如何使用编程工具对数据变量的正确使用进行仔细检查和校验。需论述的其他特征包括内存映射、检验状态标志和检验输入值的有效性。

作为安全手册的一部分或者作为应用的特殊文档，还提供给程序员小组生产类似格式和样式的程序的说明和示例。这些说明应包含程序中并不使用的特殊算法或功能的详细说明，因为这些算法或者功能可能会产生影响安全的不可预料的行为。

应告诫程序员不要作任何超出安全手册定义之外的假设，例如，不能使用安全手册中省略掉的编译器功能。理想情况下，为了增强这些限制也许已经对编译器作了配置。

一个典型的安全手册编排方式和内容的示例

表1是手册编排方式图和内容的示例，它符合GB/T 21109的典型逻辑解算器安全手册的示例。此例显示了各章的主要内容及标题。

表1 典型的安全手册编排方式和内容

章	主 要 内 容
引言	一般信息、设备要求、手册编排方式、规定、相关文档集、版本历史、术语、产品概述
安装	现场计划编制环境、过程连接、启动规程、停机规程、应用修改、已运转系统中功能的实现
配置和应用构建	设计考虑[a]、功能和性能、辅助教材
运行时间操作	产品操作、操作概述、操作说明
维护	预防性维护、硬件指示器、误差信息、应用和系统报警、故障查找和用户修理
附录	系统信息、检验表、应用解决方案
索引	安全信息索引

[a] 设计考虑规定了与PE逻辑解算器的安全配置和编程有关的配置和应用编程方面的所有问题。它们包括但不限于：

——逻辑解算器处理时间、I/O更新速率、通信速率、逻辑解算器运算顺序；

——系统报警处理要求；

——配置和编程约束。

12.4.4.8 见GB/T 21109.1。

12.4.5 开发应用软件的要求

在开发应用软件之前，应检验下列各项：

——SIS逻辑解算器及其相关的I/O模块应符合GB/T 21109.1。

——在逻辑解算器厂家发布的用户文档集或者一些文档中应提供必需符合GB/T 21109.1的所有限制和操作规程。通常把这些文档称为安全手册。

——使用可编程电子的传感器和最终元件应符合GB/T 21109.1。

——当执行定期在线测试时，应提供维护超驰能力用以测试传感器和最终元件。

通常情况下应使用逻辑解算器供应商或智能现场装置供应商提供的编程语言来编写应用软件。使用比如指令表或者C语言这些全可变语言(FVL)、比如功能块图或者梯形图这些有限要变语言(LVL)或者在用户只录入固定程序所需的数据时使用的固定程序语言(FPL)就能编写应用程序。

如用FVL编写应用软件，开发者应遵从GB/T 20438.3—2006中的要求和指南。如果采用LVL或者FPL编写应用软件，那么应遵从GB/T 21109.1的要求和指南。开发者还应遵从安全手册中逻辑解算器厂家提供的限制和规程。如果需要，还要编制编程指南和编码/配置规则。

12.4.5.1 见GB/T 21109.1。

12.4.5.2 见GB/T 21109.1。

12.4.5.3 应用程序全局变量的例子可以是一个安全报警，比如高温报警，此报警可根据过程中批的成分而改变。

应用程序全局常量的例子可以是在火灾和气体保护系统中使用的高易燃气体报警值，例如20% LEL(爆炸下限)。

12.4.5.4 见GB/T 21109.1。

12.4.5.5 见GB/T 21109.1。

12.4.5.6 见GB/T 21109.1。

12.4.6 应用软件模块测试要求

对照在设计和要求规范阶段中产生的规范，应用软件测试最初发生在一个模拟器上，然后发生在逻辑解算器硬件上。初始测试阶段(对照设计规范进行模拟和测试)的目的是：

——证明软件模块可提供必要的功能并且不会有任何违规行为；

——给该软件设置很宽的条件和序列范围，从而使其能灵活应对意外行为。

测试后继阶段(集成测试和工厂验收试验)的目的是为了证明应用软件在定义的时间关系范围内已达到它对规定的硬件的要求。

最终测试阶段，即是证明在预定的环境中，随同预定的实际装置和接口一起，并使用所定义的操作规程能正确工作的集成系统，只有在系统安装和调试运行的期间才能全部完成。

从正式测试开始，软件功能和配置数据的所有更改应严格按照所制定的修改规程执行。

12.4.6.1 见GB/T 21109.1。

12.4.6.2 见GB/T 21109.1。

12.4.6.3 见GB/T 21109.1。

12.4.7 应用软件集成测试要求

12.4.7.1 见GB/T 21109.1。

12.4.7.2 见GB/T 21109.1。

12.4.7.3 见GB/T 21109.1。

12.5 应用软件与SIS子系统的集成

12.5.1 目的

12.5.1.1 见GB/T 21109.1。

12.5.2 要求

12.5.2.1 可以在SIS确认之前的任何阶段实现集成测试。

12.5.2.2 见GB/T 21109.1。

12.5.2.3 见GB/T 21109.1。

12.6 FPL和LVL软件修改规程

12.6.1 目的

12.6.1.1 见GB/T 21109.1。

12.6.2 修改要求

应尽可能避免对安全仪表系统进行在线修改。如需在线修改则应根据安全计划对整个规程进行文档化和审批。

对于可编程安全仪表系统的所有改变，建议执行以下过程：

a) 计划编制和确定资源

应对用于修改一个可编程安全仪表系统到适当的层次上的程序进行管理、计划和确定资源，以保证更改的安全实现。

b) 影响分析

对要求的修改需要进行一次充分的危险和风险评估，包括评估对系统未更改部分的所有可能的影响(安全影响分析)。

c) 设计

修改设计应伴随整个生命周期过程，正如GB/T 21109.1中所描述的那样。

d) 验证

在更改安装之前，应完成对硬件和应用软件的全部离线验证。

在能够清楚描述和控制软件更改范围的情况下，在调试运行之前只需对所描绘的那些应用软件进行验证。

e) 安装和调试运行

更改安装和调试运行应遵循GB/T 21109.1中为安全仪表系统的安装和调试运行所制定的规程。

f) 验收测试确认

对系统的修改部分进行联机之前应对系统的修改部分进行一次系统确认(因果测试)。

g) 人员

根据人员所受培训和它们具有的经验,只有那些被证明能胜任执行修改的人,才被授权执行修改。

h) 离线修改

当对应用软件进行离线修改时,应验证所使用的应用软件的正确版本,包括操作参数。

12.6.2.1 见GB/T 21109.1。

12.7 应用软件验证

12.7.1 目的

12.7.1.1 见GB/T 21109.1。

12.7.1.2 见GB/T 21109.1。

12.7.2 要求

应用软件安全要求规范应包括:

——仪表安全功能要求(例如仪表安全功能的SIL,逻辑流程图/因果图);

——定时约束(例如输入到输出的最小响应时间);

——结构约束(例如冗余要求、通信接口和功能分离)。

验证应保证在应用软件开发的每个阶段都能满足规定的要求。

数据验证包括证实应用软件中使用的数据的正确性,并且在惟一性方面是恰当的(例如给工位名(TAG)分配惟一的名称、数据不会被其后的功能误用以及诸如报警设定点这样的常数是有效和正确的)。

防止未经授权更改的验证包括验证存在这些机制(例如带有存取级别的口令保护)和验证已充分使用了这些机制。

12.7.2.1 见GB/T 21109.1。

12.7.2.2 见GB/T 21109.1。

12.7.2.3 在应用软件开发周期(包括测试)的每个不同阶段,验证这些阶段已成功完成。通常应由一个或几个人组成的验证小组来完成验证。

为了减少因先入为主产生的误差,验证应包括:

——对SIL 1而言,应由应用程序开发小组的另一成员进行一次同级复审;

——对SIL 2而言,应由不属于应用程序开发小组的一位成员进行一次同级复审;

——对SIL 3而言,应由一个独立部门的成员进行同级复审。

在软件开发工具包含一些自动验证操作(例如检验重复使用工位名(已命名变量))的情况下,验证小组应证实那些工具已被正确使用并已得到正确的结果。

对所有的SIL来说,建议测试覆盖率包括所有应用软件的SIF以及SIS失效响应(例如电源失效、处理器失效、输入硬件失效、输出硬件失效和通信失效)。但对较高SIL而言,为了进一步减少在软件中残留的误差,建议执行以下附加测试:

——对于SIL 2和SIL 3而言,应根据内部结构(例如内部算法、内部状态)进行测试;

——对于SIL 3而言,应进行应力测试(例如,输入变量和内部变量的异常范围条件、输入的异常组合、异常时序和加载。)

对于所有SIL,建议验证和测试文档应足以能显示验证和测试已被执行并已取得成功。但对于较

高的 SIL,还建议:

——对于 SIL 2 和 SIL 3 而言,文档应足以允许对验证和测试的充分程度进行一次评估;

——对于 SIL 3 而言,文档应足以允许一个独立的人能重复这些测试和复审所达到的覆盖率。

12.7.2.4 见GB/T 21109.1。

13 工厂验收测试(FAT)

13.1 目的

13.1.1 见GB/T 21109.1。

13.2 建议

13.2.1 虽然进行一次工厂验收测试(FAT)不是必须的,但建议对于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)的仪表安全功能的逻辑解算器仍应进行一次 FAT。

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应查看的内容。

操作过程的人员应参加 FAT,因为此测试会对它们进行操作 SIS 的某些初步培训。通常,它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。

13.2.3 见GB/T 21109.1。

13.2.4 见GB/T 21109.1。

13.2.5 在 FAT 期间,应测试接口(例如 BPCS 和 SIS 之间的通信接口)。

13.2.6 见GB/T 21109.1。

13.2.7 见GB/T 21109.1。

14 SIS 安装和调试运行

14.1 目的

14.1.1 见GB/T 21109.1。

14.2 要求

14.2.1 见GB/T 21109.1。

14.2.2 应按设计和安装计划安装 SIS。项目组应正确审查 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,应对 SIS 进行充分地调试运行,并启动确认活动。

14.2.3 尽管GB/T 21109.1已把调试运行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。

14.2.4 见GB/T 21109.1。

14.2.5 见GB/T 21109.1。

15 SIS 安全确认

15.1 目的

15.1.1 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。应在 SIS 投入运行之前完成确认活动。

15.2 要求

15.2.1 见GB/T 21109.1。

15.2.2 见GB/T 21109.1。

15.2.3 见GB/T 21109.1。

15.2.4 如果 SIS 已通过 FAT,那么在确认过程中,这可能应被考虑。确认组应审查 FAT 的结果,以确保成功地测试了所有的应用软件,并且纠正了 FAT 过程中发现的所有问题。

在最终确认时，不必重复测试应用软件，这要求满足下列所有条件：

——预先考虑过这种方法，并且在确认计划编制中包含此方法；

——在 FAT 期间，应用软件已被验证是满足安全要求规范的；

——验证应用软件版本与在 FAT 时测试的版本相同。

然而，确保不存在装运/存放/吊装损伤、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。因为逻辑解算器和最终元件的分离测试并不等于整体的端对端检验测试，所以为了声明 SIS 确认，强烈推荐进行一次等效的检验测试。

15.2.5 见GB/T 21109.1。

15.2.6 见GB/T 21109.1。

15.2.7 见GB/T 21109.1。

15.2.8 见GB/T 21109.1。

16 SIS 操作和维护

16.1 目的

见GB/T 21109.1。

16.2 要求

16.2.1 见GB/T 21109.1。

16.2.2 见GB/T 21109.1。

16.2.3 见GB/T 21109.1。

16.2.4 见GB/T 21109.1。

16.2.5 见GB/T 21109.1。

16.2.6 见GB/T 21109.1。

16.2.7 见GB/T 21109.1。

16.2.8 见GB/T 21109.1。

16.3 检验测试和检查

16.3.1 检验测试

16.3.1.1 为了达到安全要求规范中规定的要求时的平均失效概率，应选择检验测试间隔。

16.3.1.2 见GB/T 21109.1。

16.3.1.3 检验测试频率应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、增加的诊断覆盖率和鲁棒部件。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 SIL 1 的系统，$PFD_{avg}=10^{-1}$；对 SIL 2 的系统，$PFD_{avg}=10^{-2}$）。

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厂商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、部件和诊断覆盖率。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，应对 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。

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

注：在考验终端脱扣元件不可行的情况下，编写的规程应包含：

a) 在单元停机期间测试最终元件。

b) 在在线测试期间，尽可能通过考验输出(例如输出脱扣继电器、关停电磁阀、阀门部分行程)来测试SIS。

c) 在计算SIF的PFD_{avg}时，应考虑最终元件测试周期的任何限制。

16.3.1.4 见GB/T 21109.1。

16.3.1.5 见GB/T 21109.1。

16.3.1.6 见GB/T 21109.1。

16.3.2 **检查**

如GB/T 21109.1中所述，检查SIS不同于检验测试。尽管检验测试可确保SIS运转正常，但都需要通过目测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。

16.3.3 **检验测试和检查的文档**

对已发现问题的记录进行的检验测试和检查得出的结果进行归档是重要的。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，以便查看部件是否存在失效历史，通常应保存足够长的时间。

例如，当一个传感器使一次检验测试失败时，良好惯例是审查以往检验测试的结果，以便查看在前几次测试中该传感器是否也曾使类似的一次检验测试失败过。如果历史表明重复的失效，则应考虑使用不同类型的传感器重新设计SIS。

17 SIS修改

17.1 目的

见GB/T 21109.1。

17.2 要求

17.2.1 见GB/T 21109.1。

17.2.2 见GB/T 21109.1。

17.2.3 见GB/T 21109.1。

17.2.4 见GB/T 21109.1。

17.2.5 见GB/T 21109.1。

17.2.6 见GB/T 21109.1。

18 SIS停用

18.1 目的

见GB/T 21109.1。

18.2 要求

18.2.1 见GB/T 21109.1。

18.2.2 见GB/T 21109.1。

18.2.3 见GB/T 21109.1。

18.2.4 见GB/T 21109.1。

18.2.5 见GB/T 21109.1。

19 信息和文档要求

19.1 目的

19.1.1 见GB/T 21109.1。

19.2 要求

19.2.1 可用来实现一个 SIS 的信息和文档清单包括：

a) 危险和风险评估的结果；
b) 在确定安全完整性等级时使用的假设；
c) 安全要求规范；
d) 应用逻辑；
e) 设计文档；
f) 修改信息和/或文档；
g) 验证和确认的记录；
h) 调试运行和 SIS 确认规程；
i) SIS 操作规程；
j) SIS 维护规程；
k) 检验测试规程；
l) 评估和审核结果。

19.2.2 见GB/T 21109.1。

19.2.3 见GB/T 21109.1。

19.2.4 见GB/T 21109.1。

19.2.5 见GB/T 21109.1。

19.2.6 见GB/T 21109.1。

19.2.7 见GB/T 21109.1。

19.2.8 见GB/T 21109.1。

19.2.9 见GB/T 21109.1。

附 录 A
（资料性附录）
计算一个仪表安全功能要求时的失效概率的技术示例

A.1 概述

本附录描述了用于计算根据GB/T 21109.1设计和安装的安全仪表系统的失效概率的许多技术。此信息的性质是资料性的，不应被解释为可能被使用的惟一的评价技术。

涉及到的方法来自GB/T 20438.6—2006的附录B、IEC 61078、IEC 61025、IEC 61165和ISA TR 84.00.02系列标准。

A.2 可靠性框图技术

IEC 61078和GB/T 20438.6—2006的附录B说明了用于计算根据GB/T 21109.1和本部分设计的仪表安全功能的失效概率的可靠性框图技术。

A.3 简化方程技术

ISA TR 84.00.02-2说明了用于计算根据GB/T 21109.1和本部分设计的仪表安全功能的失效概率的简化方程技术。

A.4 故障树分析技术

IEC 61025和ISA TR 84.00.02-3说明了用于计算根据GB/T 21109.1和本部分设计的仪表安全功能的失效概率的故障树分析技术。

A.5 马尔可夫(Markov)建模技术

IEC 61165和ISA TR 84.00.02-4说明了用于计算根据GB/T 21109.1和本部分设计的仪表安全功能的失效概率的马尔可夫建模技术。

附 录 B
（资料性附录）
典型的SIS结构开发

B.1 背景

B.1.1 引言

下面提供的示例说明了开发满足GB/T 21109.1要求的SIS结构的各个步骤。SIS工程遵循如下所述的指南和惯例，并使用标准化设备。

B.1.2 指南和惯例

在过去，安全应用被称为“关键仪表系统”。已开发了一些工程准则、典型示例、最佳惯例以及测试规程。

已存在某些使用保护层分析（如同GB/T 21109.3—2007附录F中的LOPA）、仪表冗余和设计惯例来确定要求的仪表安全功能和SIL的指南。

B.1.3 仪表

在安全应用（SIS）中，仪表使用厂家提供的诊断和安全失效分数（SFF）信息以及从应用收集到的性能信息来计算要求时的失效概率（PFD）。

B.1.4 逻辑解算器

逻辑解算器的硬件、系统软件和开发系统都是符合GB/T 20438—2006的SIL 3等级的，并且使用了用于应用程序的有限可变语言。

系统安全手册给出了有关系统应用和应用软件开发的详细指南。

用户可定义的标准安全功能（例如变送器故障检测、如1oo2、1oo3这样的冗余选择以及输出安全超驰）可作为应用程序模板被提供。模板由用户编写。

B.2 工作过程

B.2.1 引言

所有工程活动都应遵循预先定义的整个项目的工作过程。SIS的开发有它自己的过程。各个步骤都被映射到整体过程中。在适当阶段执行功能安全评估。

B.2.2 典型的SIS生命周期步骤

开发SIS应用要求的典型步骤见表B.1。下面只讨论第3步、第4步以及第5步中与系统结构有关的那些部分。

表B.1 典型的SIS生命周期步骤

步 骤	标 题	活 动
1	应用范围	定义过程设备
2	过程设备的功能安全要求	定义潜在的危险，执行保护分析等级（LOPA）
3	系统安全要求分配	设计SIS结构
4	在SIS中分配安全要求	确定SIS硬件
5	应用软件开发	设计SIS软件
6	应用软件测试和确认	测试SIS
7	安装	现场安装
8	调试运行	整体验收
9	运行	运行过程

B.2.3 安全要求分配

从 LOPA 得到的可用信息:SIS 应用的安全要求规范和 SIL(例如每个 SIF 的 SIL)。

用于实现 SIL 的模型:见图 B.1。

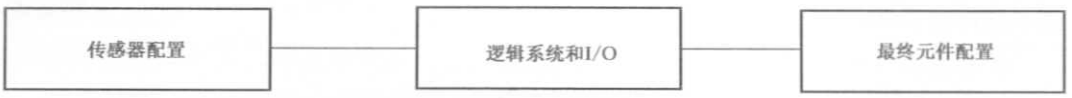


图 B.1 实现 SIL 使用的模型

确定 PFD:所有 PFD(见上)要求在 SIL 限制内。

简化方法:在与 SIL 要求相关的表中,可提供包括冗余类型(如 1oo2)、可用的诊断和测试间隔在内的标准仪表配置。这些表以设施内的各种过程应用的经验数据和经检验过的设计为基础。把可选的系统配置与已知元素数据组合起来,并连接到方框图,使之能选择最合适的方案。

SIS 部件规范:正如GB/T 21109.1中所要求的那样,所有系统部件都具有已验证的特性(如对规定的 SIL 的 PFD、SFF、故障裕度和系统要求)。

——传感器和最终元件:已针对过程应用对它们作了适当地选择,并且工程部门根据操作经验对各种类型的特征进行了标准化。

——逻辑系统:应根据传感器和最终元件要求来规定 I/O。逻辑解算器、应用语言、开发工具和通信接口都是被认可的安全系统的组成部分。操作员接口应能根据应用要求进行调整。

B.2.4 在 SIS 内分配安全要求

在这一步骤中,应把安全要求规范的所有功能分配给系统部件、功能或软件。安全完整性要求应确定合适的 SIS 部件和可能的 SIS 结构。

B.2.5 应用软件要求相关的结构

在选择 SIS 结构之后,正如对传感器、逻辑解算器和最终元件所要求的那样,为了实现冗余(例如 1oo2)和/或诊断,可能不得不规定应用软件。

B.2.6 应用软件开发

编程语言是功能块图(一种有限可变语言)。代码编写和测试是一个众所周知的过程。此外,对于系统安全手册中详细描述的安全功能编程有某些限制。

B.3 示例 1

B.3.1 概述

下面的示例并非一个真实的情况,它并未考虑与其他安全层的共同原因失效。特别编写此示例来说明如何应用上述的 SIS 设计过程。

B.3.2 危险情况

蒸汽加热反应器的温度控制出现故障,并完全打开蒸汽控制阀。

B.3.3 SRS 和 SIL

安全要求规范:当反应器压力超过 10 bar 时,在 20 s 内关闭到反应器汽套的蒸汽,以避免发生放热反应。不需要操作员动作。要求的 SIL 为 3。

B.3.4 系统结构

系统部件:压力传感器配置、逻辑解算器配置、最终元件配置。经使用检验过的智能传感器直接与逻辑系统的输入相连。应急闭锁阀已同电磁阀集成在一起,并直接与逻辑系统的输出相连。所有的 MTTF 数据都来自实际操作经验。

可用的仪表:

——压力传感器符合GB/T 21109.1—2007的 11.4.4:MTTF=1×10^5 h,DC=70%,SFF=90%,检验测试间隔为每年,MTTR=8 h;

——应急闭锁阀符合GB/T 21109.1—2007的 11.4.4:MTTF=8×10^4 h,DC=0%,SFF=60%,检验测试间隔为每 6 个月,MTTR=8 h。

单个元件的 PFD:

——传感器:2.2×10^{-3}(见 A.1)——不可接受;

——逻辑解算器(冗余的):1.3×10^{-4},包括 I/O 接口(来自认证);

——阀门:2.41×10^{-3}(见 A.1)——不可接受。

求出可接受的传感器结构:选择 1oo2 冗余。

共同原因=10%,DC=90%(见 A.1)。

1oo2 传感器结构的新 PFD=2.3×10^{-4}。

检验GB/T 21109.1—2007的表 6 和 11.4.4,实际故障裕度=1→SIL 3——可接受。

求出可接受的最终元件结构:选择 1oo2 冗余。

共同原因=10%(见 A.1)。

1oo2 最终元件结构的新 PFD:4.65×10^{-4}。

检验GB/T 21109.1—2007的表 6 和 11.4.4,实际故障裕度=1→SIL 3——可接受。

PFD 检验:传感器+逻辑解算器+最终元件。

$(2.3+1.3+4.7)\times10^{-4}=8.3\times10^{-4}<10^{-3}$。

B.3.5 安全软件相关的附加结构

传感器配置软件:对于 1oo2 以上的传感器,信号选择软件被编程(现有功能块)来关闭蒸气阀,如果:

——两个传感器中的一个读到超过所规定的过程值的状况;

——诊断揭露出一个危险失效。

最终元件配置软件:在安全程序命令一个安全输出动作的情况下,两个蒸汽阀的输出都被断电。

B.4 示例 2

B.4.1 概述

导致较低 SIL 结果的类似例子。

B.4.2 危险情况

蒸汽加热反应器的温度控制出现故障,并完全打开蒸汽控制阀。

B.4.3 SRS 和 SIL

安全要求规范:当间歇式反应器压力超过 10 bar 时,在 20 s 内关断给反应器馈送反应物"A",以避免放热反应。不需要操作员动作。要求的 SIL 为 2。

B.4.4 系统结构

系统部件:压力传感器配置、逻辑解算器配置、最终元件配置。经使用检验过的智能传感器直接与逻辑系统的输入相连。应急闭锁阀已同电磁阀集成在一起,并直接与逻辑系统的输出相连。所有的 MTTF 数据都来自实际操作经验。

可用的仪表:

——压力传感器符合GB/T 21109.1—2007的 11.4.4:MTTF=1×10^5 h,DC=70%,SFF=90%,检验测试间隔为每年,MTTR=8 h;

——应急闭锁阀符合GB/T 21109.1—2007的 11.4.4:MTTF=2.5×10^4 h,DC=0%,SFF=60%,检验测试间隔为每周(168h),MTTR=8 h。

单个元件的 PFD:

——传感器:2.2×10^{-3}(见 A.1)——可接受。

——逻辑解算器(冗余的):1.3×10^{-4},包括 I/O 接口(来自认证)。

——阀门:见下(公式见 A.1)。

单个传感器的 PFD:

1oo1 传感器结构的 PFD:2.2×10^{-3}。

检验GB/T 21109.1—2007的表 6 和 11.4.4,实际故障裕度=0→SIL 2——可接受。

单个最终元件的 PFD:(公式见 A.1)

$PFD=\lambda_D\times t_{CE}$,$\lambda_D=1/(25\ 000\times2)$,$t_{CE}=168/2+8$。

1oo1 最终元件结构的 PFD=1.84×10^{-3},检验GB/T 21109.1—2007的表 6 和 11.4.4,实际故障裕度=0→SIL 2——可接收。

PFD 检验:传感器+逻辑解算器+最终元件。

$(2.2+0.1+1.8)\times10^{-3}=4.1\times10^{-3}<10^{-2}$。

B.4.5 安全软件相关的附加结构

最终元件配置软件:当安全程序命令一个安全输出动作时,蒸汽阀输出就被断电。

此外,编写监视软件来验证每当阀门被操作时(每批一次,典型地每 8 h 一次),阀门就达到安全状态。当测试失效,或者如果从最后一次测试起经过的时间大于 168 h,则逻辑解算器输出保持在安全状态(应急闭锁阀门关闭),且工况被报警。这种自动测试允许在计算 PFD 时,设置检验测试间隔为 168 h。

附 录 C
（资料性附录）
安全 PLC 的应用特征

本附录描述了在 SIS 应用中使用小型的(如 I/O 小于 150)安全 PLC 时，集成商应考虑的一些关键步骤。它被用于在初始设计计划时给标准使用者提供帮助。

安全 PLC 是一个符合GB/T 20438—2006的经认证过的 SIS 逻辑解算器。对于一个特殊的安全应用而言，传感器和最终元件分别被连接到 SIS 逻辑解算器的 I/O 端并且应用程序被实现。涉及 SIS 逻辑解算器失效的所有安全功能性(如在线检查、时间控制)都是嵌入式系统的组成部分。在应用软件的范围内实现对传感器和最终元件所必需的检验；对某些功能而言，存在经认可的功能块。

存在所有装置的安全完整性数据(例如 PFD、SIL 声明限值等)。在逻辑解算器手册中给出了逻辑解算器的安全完整性数据。

C.1 系统

SIS 逻辑解算器是一个 PLC，它是专门为安全应用而设计的，见图 C.1。它的型式认证符合 GB/T 20438—2006，并达到最高 SIL 3 等级。它有用于安全相关过程信号以及同其他的安全 PLC 通信的输入和输出接口。它也有供非安全相关过程信号以及同其他非安全 PLC 通信的接口。系统包括：

——具有功能安全的特殊硬件特征的 CPU、一个特殊的操作系统和用来控制失效的嵌入式功能(对于应用程序编程和软件集成而言，集成的冗余是由开发系统支持的。程序员只看一个 CPU)；

——用于有限可变语言(如功能块图)的开发系统；

——具有经认可的功能块的程序库；

——仪表安全功能参数的专用配置工具；

——用来证实被下载的运行时间应用软件和源应用软件相同的工具；

——安全手册。

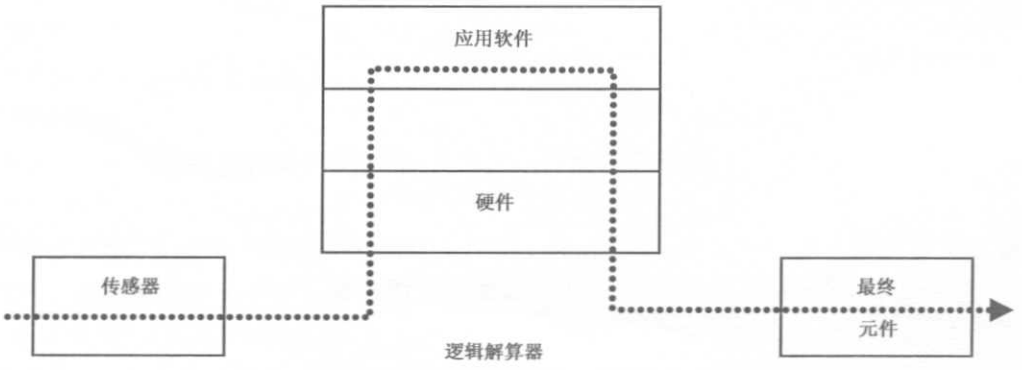


图 C.1 逻辑解算器

C.2 工作过程

a) 安全要求规范应符合本部分：下面是一些关键的考虑：

1) 所有仪表安全功能的规范；

2) 模拟输入的范围；

3) 传感器和最终元件在线诊断的定义；

4) 在检测到的失效模式下系统反应的描述；

5) 仪表安全功能参数(例如最大周期、对比输入的最大允许时间差)的定义；

6) 安全手册中的限制。

b) 应用软件安全要求规范应该是从 a)派生出来的。

在安全手册中描述了论及逻辑解算器硬件(PLC)的安全要求。约束主要描述比如性能极限、内存容量、响应时间这些项目。

在安全手册中描述了软件结构的约束和代码实现。它们描述 PLC 的开发系统。大多数约束都是由有限可变语言隐式给出的。

c) 应用软件结构设计：应用结构设计应详尽地反映出为过程所规定的仪表安全功能和操作模式。

d) 应用软件开发：使用现有的功能块可简化应用软件开发。

e) 集成：集成包含下载配置数据(如 I/O 表)、应用软件和所有的参数设定值，这些设定值与默认设定值不同。

f) 验证：在集成系统之前或者之后都应对应用软件进行验证。验证应由开发环境支持。

附 录 D
（资料性附录）
SIS 逻辑解算器应用软件开发方法的示例

本例说明了一个特定的 SIS 逻辑解算器集成商怎样为他的客户开发安全应用软件。典型地，开发此软件被当作整个系统集成过程的一部分，在下面将被讨论。

因为强调的重点是应用软件开发方法，所以讨论开发应用软件曾使用的软件开发工具、编程语言和编码标准是很重要的。讨论的目的是提供软件开发工具的典型特征、在一个 SIS 逻辑中所提供的编程语言和相关的语言翻译器的一个示例。

SIS 逻辑解算器具有支持许多GB/T 15969.3语言的应用编程软件开发工具。GB/T 15969.3定义了许多可编程逻辑控制器通用的语言。因为GB/T 15969.3标准并未论述安全应用，所以决定：

——使用有限可变语言作为过程领域的通用语言；

——去掉不适合于安全应用的语言结构；

——使用一个代码标准以进一步限制关键应用时语言结构的使用；

——增加访问保密和文件保护特征；

——提供GB/T 15969.3功能、功能块的经认证过的程序库以及与功能有关的过程（如模拟数据处理、火灾和气体传感器）；

——提供应用编程软件开发工具、程序库和语言翻译器的第三方认证。

关于应用开发软件的这些决定在 D.2 中作了更详尽的描述。

在 D.3 中还描述了 SIS 逻辑解算器程序员所使用的代码标准的一个示例。应考虑的软件开发工具的附加要求见 D.4。

D.1 整体系统集成过程的概述

配备有 SIS 逻辑解算器的安全仪表系统的主要集成服务包含许多活动：

a) 硬件集成

它包括把 SIS 逻辑解算器装入机柜，这个机柜带有用来把过程信号连接到逻辑解算器 I/O 模块的端子板。通常还包括逻辑解算器的电源和配电。

b) 应用逻辑定义

通过与买方工程师紧密配合，SIS 逻辑解算器集成服务也可定义详细的逻辑。定义每个仪表安全功能的应用逻辑应考虑传感器和最终元件的冗余。为了满足买方的操作要求，还定义了在过程运行的同时进行测试和维护 SIS 的接口。也包括了附加的非安全关键逻辑，但这种逻辑应按安全功能同样的标准被严格地分离和设计。

c) 应用软件实现和硬件配置

经认证过的 SIS 逻辑解算器的应用软件开发软件包被用来配置 SIS 逻辑解算器 I/O 和通信硬件。每个仪表安全功能的应用软件以及非关键应用软件也都被实现和测试。

d) 工厂验收测试

在发货到工厂之前，许多买方都要进行一次工厂验收测试，以便检验硬件和应用软件的正确运行。买方工程师和其他操作人员应彻底测试硬件和应用软件。

e) 在买方现场安装 SIS

供货商应提供现场安装或安装监督。

f) 现场验收测试

应检验每个传感器和接入 SIS 逻辑解算器的接口的正确运行和校准。应重新测试比如整

体应用软件、维护用的旁路功能这些项目。

g) 应用软件和硬件修改

在初始安装和运行之后，应使用严格的工厂认可的修改规程对应用软件和硬件进行修改。

D.2 SIS 逻辑解算器开发软件

如前面所述，SIS 逻辑解算器使用一个基于GB/T 15969.3语言的应用软件开发软件包。该软件支持GB/T 15969.3的 3 种语言：结构化文本、梯形图和功能块。分离每种语言的代码标准是必要的。不包含指令表，因为这些语言类似于汇编语言，且不适合于应用程序员。这是同 GB/T 20438.7—2006 的表 C.1 一致的。对同GB/T 20438.3—2006的 7.4.4 和表 A.3 以及 GB/T 20438.7—2006 的 C.4 中描述的要求一致的GB/T 15969.3语言定义附加了许多限制。这些限制包括：

a) GB/T 15969.3 定义了 20 种数据类型（BOOL、SINT、INT、DINT、LINT、USINT、UINT、UDINT、ULINT、REAL、LREAL、TIME、DATE、TOD、DT、STRING、BYTE、WORD、DWORD、LWORD）。注意，只有 8 种整型数据类型。所有这些数据类型的支持还需要许多种变换和截断函数的支持。对安全应用来说这些数据类型中的许多类型是不必要的。所支持的数据类型的数目被限于 11 种。对于特定的语言所提供的数据类型选项只有 8 种：BOOL、INT、DINT、DWORD、REAL、LREAL、STRING、TIME、DATE、TOD 和 DT。这种决定是同限制语言子集的GB/T 20438—2006建议（见GB/T 20438.3—2006中的表 A.3）一致的。

b) 不支持使用GB/T 15969.3的图形执行控制元素（如无条件转移、条件转移、无条件返回和条件返回），因为它们会导致应被执行的元素的循环和非预定的旁路（见 GB/T 20438.7—2006 中的 C.4.6）。

c) 不支持许多结构化文本语句，因为它们会引起循环（如 FOR…END_FOR、WHILE…END_WHILE 和 REPEAT…END_REPEAT）。

d) 加强了一个限制从而使得语言不允许多个程序写入同样的全局变量。许多程序可以读某个全局变量，但为了防止冲突和覆盖，一个程序只能写入一个全局变量。此外，如果编程时无意中进行了多重写入，应用编程软件将产生一次警告。

e) 编程软件应无歧义地定义程序中所有元素的执行次序。有些语言具有一种确定每个可执行的元素的执行次序的算法，并显示执行次序的能力。

f) 编程软件应保证安全关键软件和非安全关键软件的分离。该软件为程序员提供了定义安全程序和非安全程序的能力。编程软件还提供了定义安全变量和非安全变量的能力。非安全程序不能写入安全变量。

g) 已发现对大多数应用用户而言，使用 VAR_IN_OUT 变量是十分含糊不清的。使用 VAR_IN_OUT 变量需要非常彻底的文档化，或者编程语言不应支持它们。

D.3 应用程序员的编码标准

为了保证安全应用软件的开发，应确立应用程序员的编码标准。下面是供应用程序员在利用特殊的开发软件来开发应用软件时使用的指南：

a) 应用程序员应使用有限可变语言（功能块图或梯形图）来实现仪表安全功能。甚至还应限制这些语言（见上面关于语言子集的 D.2）。

b) 结构化文本（ST）是一种全可变语言，它的使用应受到限制。只要可能，应限制为用于功能和功能块的实现。实行这种限制从而使得并不精通编程的操作人员也能理解安全程序。

c) 程序大小应限制到一个合理的大小。不同过程单元的仪表安全功能应处在一些分开的程序之中。理想地，一个程序应只包含一个过程单元的少数几个仪表安全功能。

d) 应避免混淆。例如,如果编程软件支持数组,使用数组的程序应检验数组指针以确保它们在有效范围之内。

e) 当应用程序包含非安全关键逻辑以及安全关键逻辑时,非安全关键逻辑应处在一些分开的程序之中并利用程序中所并入的一些分离规则。

D.4 安全应用时的配置/编程和运行期系统的其他要求

应用编程软件提供了许多允许用户存取SIS逻辑解算器信息的特征。但有必要保证所开发的软件的保密性以及允许用户检验软件的正确的运行。下面描述了几个这样的特征:

a) 编程软件提供了一个保密系统,这个系统把所有的用户限定为只有那些职责与其职务相称的人(如公司经理、现场经理、项目经理、项目工程师、高级程序员、程序员、操作员)。每个用户的姓名和口令登录到系统中,并且每个用户只能在分配给它们的功能级上工作。保密系统还提供了一个用于安全编程的用户级并且为非安全编程提供另外一个用户级,因为用户公司希望把在现场更改安全程序限定为极少几个人。

b) 提供有被保护或被锁定的功能和程序库,程序员不能访问或更改它们。这保证了已经被认证或充分测试过的程序库不会被修改,除非一个正式的修改申请已得到批准。保密系统允许用户定义可访问和更改程序库的高层人员(典型的是公司经理或者现场经理)。

c) 编程软件还提供了正被开发的项目中所有元素的版本号。系统配置、功能、功能块、或程序的任何改变结果都得更改该元素的版本号。这使用户可以很快地了解到它们的文档集是否已过期,并且还使得用户能把测试集中到已被更改过的那些项目上。编程软件还包含版本比较功能,它使得用户能检验所有的更改,包括无意中的更改。这些比较功能应包括全局工位名数据库和程序执行清单中的任何更改。

d) 借助对应用项目的复合文件结构中存放的所有数据流循环冗余检验的计算和检查,软件可提供文件的安全性。

e) SIS逻辑解算器提供了对其诊断信息的访问,因此程序员可根据逻辑解算器的状态采取适当的动作。

f) SIS逻辑解算器提供了一个运行时间环境,该环境提供了算术的异常处理,从而使程序员能检验正确的算术操作。

g) 编程软件提供了在编程工作站上对开发的所有程序进行仿真的能力。这使得程序员在把开发的的所有软件装入SIS逻辑解算器之前能在线检验这些软件。对于系统正在运行的同时在线更改程序的情况而言,这个特征应该是必须的。

h) 编程软件支持可用来做与仿真软件接口的DDE(动态数据交换)。这提供了能在应用软件被装入安全控制器之前对它进行附加离线测试的能力。

D.5 假设

本章描述与用来开发应用软件的硬件和软件相关的一些假设。还描述了文档集和规程。

1) SIS逻辑解算器和与它有关的I/O模块已由第三方评估,并认定符合GB/T 20438—2006。第三方授予的GB/T 20438—2006的认证范围是用于SIL 3的仪表安全功能的部件。

2) 语言是GB/T 15969.3的功能块图(FBD)、梯形图(LD)和结构化文本(ST)语言的一个有限可变子集。应用程序库中提供的所有功能和功能块都有一个属性,此属性标记了功能是作安全应用还是只作非安全应用。在应用程序中只有标记有安全属性的那些功能和功能块才能用来实现仪表安全功能。标记有非安全属性的应用程序可使用具有非安全属性和安全属性的功能和功能块。

3) 所有支持的GB/T 15969.3的编程语言和具有安全属性的功能和功能块的程序库都已按照

GB/T 20438—2006进行了符合性认证。

4) 在用户文档集中提供了认证组织的所有限制和操作规程。

5) 为了定期测试 SIS 的所有元素，一般需要一种维护超驰方法使之能在不用关闭受控过程的同时进行在线测试。

6) 使用 ISO 9000 或等同的规程执行所有的系统集成功能。

附 录 E
（资料性附录）
开发安全配置的 PE 逻辑解算器的外配诊断程序的示例

在设计 PE 逻辑解算器时，经使用验证的 PE 逻辑解算器应证明有足够的诊断能力。这些诊断功能可以是基于软件或基于硬件的功能，并且应覆盖整个逻辑解算器，包括输入模块、主处理器、输出模块和通信。

下面是可用来提供安全配置的 PE 逻辑解算器的诊断程序的一种方案。

E.1 内部配置的诊断程序

工业过程领域用的 PE 逻辑解算器内部配置有诊断程序。在本附录中它们被称为内部看门狗定时器(IWDT)。IWDT 包括软件、硬件和通信诊断子系统，它由生产厂配备在 PE 逻辑解算器内部。

SIF 应用的 PE 逻辑解算器应为 PE 逻辑解算器所有元素提供诊断。一个 IWDT 系统可为用户提供从关闭一个输入卡件或者一个输出卡件到关闭整个系统范围内的一些可选项。IWDT 诊断可检验逻辑解算器生产厂认为是最重要的那些选项。IWDT 的局限性包括：

——由与逻辑解算器相同原因引起的 IWDT 故障导致的潜在共同模式失效有可能使 IWDT 无能力执行它的诊断功能；

——(IWDT 的)实现也不能给用户提供有关逻辑解算器故障状况的诊断信息；

——无监视整个 PE 逻辑解算器，包括 I/O、主处理器和通信的能力；

——无监视应用软件模块和执行的能力。

E.2 外部配置的诊断程序

——附加在 IWDT 中的限制可能要求给执行仪表安全功能的 PE 逻辑解算器增加外部看门狗定时器(EWDT)。对于仪表安全功能来说，使用 EWDT 决不是不需要 IWDT。

——常用的 EWDT 装置的例子是旋转脉动器(rotopulsor)监视器或电子定时监视器。EWDT 的最基本形式是由 PE 逻辑解算器应用软件中的应用逻辑对它连续施加脉冲。通常使用的概念是把指令编程为几个组(这些组在内存单元中被很宽地隔开)从而产生一个具有要求周期的方波。此方波被用作 PE 逻辑至 EWDT 的输入。图 E.1 是显示 PE 逻辑解算器的脉冲式输出和 EWDT 的输出的定时图。

——此方法推动一个 PE 逻辑解算器的输出按正确的定时顺序断开和闭合，从而使 EWDT 的输出保持被加电的状态。注意，EWDT 典型地内置有可调的 ON 延迟和 OFF 延迟定时器功能。应把 EWDT 的 ON 延迟和 OFF 延迟设定值设置成无论哪种延迟都不得超时。当 EWDT 超时时，EWDT 的输出就下降，并且将关闭 SIF 和/或报警。这些方波中的脉冲可通过改变方波发生器中的应用程序加以改变。

——当执行 EWDT 诊断时应考虑的附加设计特征包括：

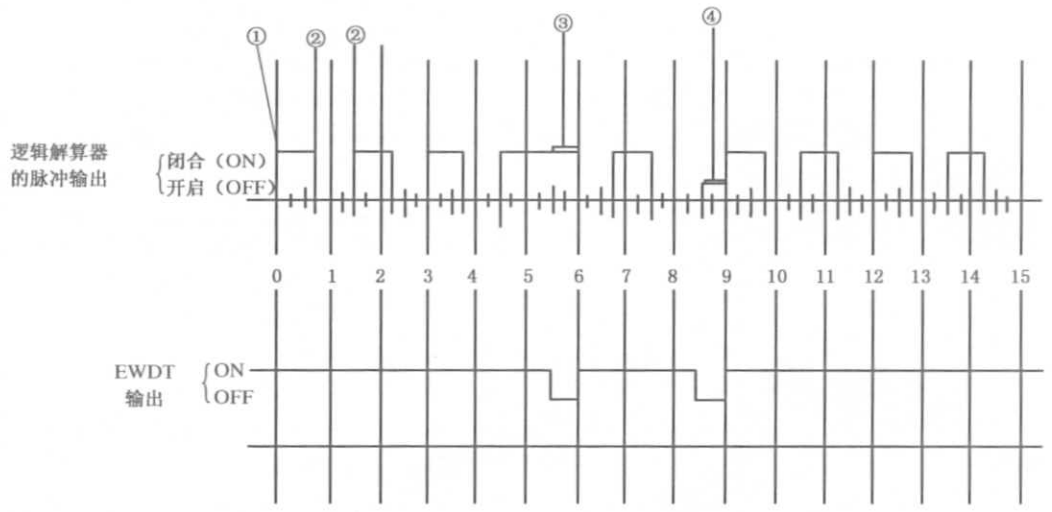
- 用于 EWDT 的 PE 逻辑解算器方波的产生，使用 SIF 应用软件使用的同一指令集。
- 专用 PE 逻辑解算器的输入被用来监视逻辑解算器输入总线状态以便检测异常运行。
- 遍及 PE 逻辑解算器的各个内存单元的 EWDT 程序的分布；这些程序能最好地监视整个存储器的功能性。
- 为提高 PE 逻辑解算器通信的诊断能力，所产生的方波在整个 PE 逻辑解算器通信系统中进行传输。
- 可能需要的复位按钮。如果在启动时 EWDT 被互锁或在关闭时被互锁，则需要一个复位

按钮。当设计复位电路时，EWDT 和 IWDT 两者都应被考虑。

- 可能需要的测试按钮。为验证 EWDT 的功能性可能需要一个测试按钮。
- 专用 PE 逻辑解算器的输出被用来监视逻辑解算器输出总线状态以便检测异常运行。
- 减少机电继电器触点产生的对电子电路的感应干扰的浪涌抑制器。应复审满足规定要求的附加电源线路的应用，比如：欠压保护，电噪声抑制，闪电保护，报警设计，从而能确定是 EWDT 启动或是 IWDT 启动。

E.3 参考

CCPS, "Guidelines for Safe Automation of Chemical Processes", AIChE, 345 East 47th Street, New York, New York 10017, ISBN 0-8169-0554-1, 1993。



① 闭合控制电路给输出加电。

② 在定时间隔(假设定为 1 s)结束之前，开启和闭合控制电路以保持给 EWDT 输出加电。只要被监视的脉动持续提供每个定时间隔至少 1 次转换，该输出就保持加电。

③ 如果被监视的控制的闭合(ON)的持续时间大于预设时间(③)，EWDT 的输出就会被断电。

④ 如果被监视的控制的开启(OFF)的持续时间大于预设时间(④)，EWDT 的输出也会被断电。

图 E.1 EWDT 定时图